NIST Special Publication 800-53
Revision 1

Recommended Security Controls for Federal Information Systems

Ron Ross
Stu Katzke
Arnold Johnson
Marianne Swanson
Gary Stoneburner
George Rogers

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

INFORMATION SECURITY

SECOND PUBLIC DRAFT

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

July 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation’s measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL’s responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL’s research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

NIST Special Publication 800-53, Revision 1, XXX pages

(July 2006) CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There are references in this publication to documents currently under development by NIST in accordance with responsibilities assigned to NIST under the Federal Information Security Management Act of 2002. The methodologies in this document may be used even before the completion of such companion documents. Thus, until such time as each document is completed, current requirements, guidelines, and procedures (where they exist) remain operative. For planning and transition purposes, agencies may wish to closely follow the development of these new documents by NIST. Individuals are also encouraged to review the public draft documents and offer their comments to NIST. All NIST documents mentioned in this publication, other than the ones noted above, are available at: http://csrc.nist.gov/publications.

THE PUBLIC COMMENT PERIOD FOR THIS DOCUMENT IS JULY 28-AUGUST 25, 2006.
COMMENTS MAY BE SUBMITTED TO THE COMPUTER SECURITY DIVISION, INFORMATION TECHNOLOGY LABORATORY, NIST VIA ELECTRONIC MAIL AT SEC-CERT@NIST.GOV OR VIA REGULAR MAIL AT
100 BUREAU DRIVE (MAIL STOP 8930) GAITHERSBURG, MD 20899-8930

Compliance with NIST Standards and Guidelines

NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programs to protect their information and information systems.

- Federal Information Processing Standards (FIPS) are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.
- Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance.[1]
- Other security-related publications, including interagency and internal reports (NISTIRs), and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when so specified by OMB.

Schedule for Compliance with NIST Standards and Guidelines:

- For legacy information systems, agencies are expected to be in compliance with NIST security standards and guidelines within one year of the publication date unless otherwise directed by OMB or NIST.[2]
- For information systems under development, agencies are expected to be in compliance with NIST security standards and guidelines immediately upon deployment of the system.

[1] While agencies are required to follow NIST guidance in accordance with OMB policy, there is flexibility within NIST's guidance in how agencies apply the guidance. Unless otherwise specified by OMB, the 800-series guidance documents published by NIST generally allow agencies some latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems. When assessing agency compliance with NIST guidance, auditors, evaluators, and/or assessors should consider the intent of the security concepts and principles articulated within the particular guidance document and how the agency applied the guidance in the context of its specific mission responsibilities, operational environments, and unique organizational conditions.

[2] The one-year compliance date for revisions to NIST Special Publications applies only to the new and/or updated material in the publications resulting from the periodic revision process. Agencies are expected to be in compliance with previous versions of NIST Special Publications within one year of the publication date of the previous versions.

Acknowledgements

The authors, Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, George Rogers, and Gary Stoneburner, wish to thank their colleagues who reviewed drafts of this document and contributed to its development. A special note of thanks goes to Peggy Himes and Elizabeth Lennon for their superb technical editing and administrative support, to Murugiah Souppaya and the NIST information security operations group for their review of the security controls and insightful recommendations, and to Annabelle Lee for her contribution to earlier versions of the document. The authors also gratefully acknowledge and appreciate the many contributions from individuals in the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

IMPLEMENTING SECURITY STANDARDS AND GUIDELINES

In accordance with the Federal Information Security Management Act of 2002, FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory, non-waiverable standard. To comply with the federal standard, agencies must first determine the security category of their information system in accordance with the provisions of FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and then apply the appropriate set of minimum (baseline) security controls in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. Agencies have flexibility in applying the minimum security controls based on the tailoring guidance provided in Special Publication 800-53. This allows agencies to adjust the security controls to more closely fit their mission requirements and operational environments.

~~If a NIST Special Publication is referenced in the Supplemental Guidance for a particular security control in Special Publication 800-53, agencies are required to follow that guidance when developing, implementing, and assessing that control. NIST guidance documents are traditionally written with a degree of flexibility in mind so agencies can apply the basic concepts in the guidance while maintaining the needed flexibility for specific operational environments and unique conditions within their organizations. This is consistent with OMB policy as articulated in the annual FISMA Reporting Guidance.~~

The combination of FIPS 200 and NIST Special Publication 800-53 requires a foundational level of security for all federal information and information systems (~~non~~ other than national security~~-related~~ information and information systems) ~~and establishes a level of "security due diligence" for federal agencies and their support contractors~~. The agency's risk assessment should validate the minimum security control set and determine if any additional controls are needed to protect ~~the~~ agency'~~s~~ operations (including mission, functions, image, or reputation), ~~and~~ agency assets, or individuals ~~including mission, functions, image, or reputation~~. The resulting set of security controls establishes a level of "security due diligence" for federal agencies and their contractors.

See http://csrc.nist.gov/sec-cert/ca-compliance.html for additional information on compliance.

Notes to Reviewers

Following the approval and publication of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, we began the biennial review and update cycle for NIST Special Publication 800-53. This biennial review and update cycle is important to ensure that the security controls listed in the control catalog and the minimum security controls populating the control baselines represent the current state-of-the-practice in safeguards and countermeasures for information systems. During the past year, we received many insightful comments from our customers on the format, structure, and content of the Special Publication 800-53. The recommendations for modifications reflect: (i) customer experience gained from employing the security controls; (ii) changing threat environments; and (iii) new technologies that are available and can impact information security. In addition to proposing necessary changes to Special Publication 800-53, it is also important to maintain a degree of stability within the publication as customers gain a better understanding of the security controls and begin to employ the controls within their organizational information systems.

NIST Special Publication 800-53, Revision 1, contains relatively modest changes in a few notable areas. First, there have been several additions to the security control catalog, reflecting new controls and control enhancements that will provide customers with greater choices in supplementing their security control baselines. Second, there have been some minor additions to the security control baselines reflecting an increased need for protection within federal information systems and to better align the minimum security controls with current federal policy and recommended security practices. Third, there have been some changes to the tailoring guidance for security control baselines reflecting environmental considerations and the application of compensating controls. Fourth, Chapters Two and Three have been expanded to include guidance on implementing security controls in external environments and responding to information system incidents. And finally, there have been two new appendices added to the publication providing; (i) a two-way crosswalk from the security controls in Special Publication 800-53 to the NIST suite of security standards and guidelines; and (ii) initial guidance on the application of Special Publication 800-53 to industrial control systems.

The relationship of NIST Special Publication 800-53 to FIPS 200 (i.e., specifying mandatory minimum security requirements and controls) makes this biennial review and update cycle critically important to federal agencies and contractors providing support to those agencies. The proposed modifications to the catalog of security controls and security control baselines will go through a rigorous, public review process to obtain government and private sector feedback and to build consensus for the changes. Comments will be accepted through August 25, 2006. Comments should be forwarded to the Computer Security Division, Information Technology Laboratory at NIST or submitted via email to sec-cert@nist.gov. General information about the FISMA Implementation Project, including all of the FISMA-related security standards and guidelines, how the FISMA publications can be used to manage enterprise risk and build a comprehensive information security program, and the organizational credentialing program under development as part of Phase II, can be found on the main web site at http://csrc.nist.gov/sec-cert.

We have attempted to provide improvements in Special Publication 800-53, Revision 1, that will help our customers effectively select and specify security controls for their information systems—and to do so, using a risk-based approach that facilitates cost-effective information security. Your feedback to us, as always, is critical in the security standards and guidelines development process to ensure that the work products produced by NIST are meeting the security needs of the federal government and the organizations in the private sector that voluntarily use these products.

-- Ron Ross
Project Leader, FISMA Implementation Project

Table of Contents

CHAPTER ONE

INTRODUCTION

THE NEED FOR SECURITY CONTROLS TO PROTECT INFORMATION SYSTEMS

The selection and employment of appropriate *security controls* for an information system[3] ~~is an~~ are important tasks that can have major implications on the operations[4] and assets of an organization as well as the welfare of individuals. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. There are several important questions that should be answered by organizational officials when addressing the security considerations for their information systems:

- What security controls are needed to adequately protect the information systems that support the operations and assets of the organization in order for that organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals?
- Have the selected security controls been implemented or is there a realistic plan for their implementation?
- What is the desired or required level of assurance (i.e., grounds for confidence) that the selected security controls, as implemented, are effective[5] in their application?

The answers to these questions are not given in isolation but rather in the context of an effective *information security program* for the organization that identifies, controls, and mitigates risks to its information and information systems.[6] The security controls defined in Special Publication 800-53 and recommended for use by organizations in protecting their information systems should be employed in conjunction with and as part of a well-defined information security program. An effective information security program should include:

- Periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization;
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each organizational information system;

[3] An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[4] Organizational operations include mission, functions, image, and reputation.

[5] Security control effectiveness addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment.

[6] The E-Government Act (P.L. 107-347), passed by the one hundred and seventh Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets.

- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization;
- Procedures for detecting, reporting, and responding to security incidents; and
- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the organization.

It is of paramount importance that responsible ~~individuals~~ officials within the organization understand the risks and other factors that could adversely affect ~~their~~ organizational operations, ~~and~~ organizational assets, or individuals. Moreover, these officials must understand the current status of their security programs and the security controls planned or in place to protect their information systems in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the organization and to accomplish the organization's stated mission(s) with what the Office of Management and Budget (OMB) Circular A-130 defines as *adequate security*, or security commensurate with risk, including the magnitude of harm to individuals, the organization, or it assets resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines apply to all components[7] of an information system that process, store, or transmit federal information. The guidelines have been developed to help achieve more secure information systems within the federal government by:

- Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems;
- Providing a recommendation for minimum security controls for information systems categorized in accordance with Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*;

[7] Information system components include, but are not limited to, mainframes, servers, workstations, network components, operating systems, middleware, and applications. Network components can include, for example, such devices as firewalls, sensors (local or remote), switches, routers, gateways, wireless access points, and network appliances. Servers can include, for example, database servers, authentication servers, electronic mail and web servers, proxy servers, domain name servers, and network time servers. Information system components are either purchased commercially off-the-shelf or are custom-developed and can be deployed in land-based, sea-based, airborne, and/or space-based information systems.

- ~~Promoting a dynamic, extensible~~ Providing a stable, yet flexible catalog of security controls for information systems to meet current organizational protection needs and the demands of future protection needs based on changing requirements and technologies; and
- Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness.

The guidelines provided in this special publication are applicable to all federal information systems[8] other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542.[9] The guidelines have been broadly developed from a technical perspective to complement similar guidelines for national security systems. This publication is intended to provide guidance to federal agencies implementing FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. In addition to the agencies of the federal government, state, local, and tribal governments, and private sector organizations that compose the critical infrastructure of the United States, are encouraged to ~~consider the~~ use ~~of~~ these guidelines, as appropriate.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse federal audience of information system and information security professionals including: (i) individuals with information system and information security management and oversight responsibilities (e.g., chief information officers, senior agency information security officers, and authorizing officials); (ii) individuals with information system development responsibilities (e.g., program and project managers); (iii) individuals with information security implementation and operational responsibilities (e.g., information system owners, information owners, information system security officers); and (iv) individuals with information system and information security assessment and monitoring responsibilities (e.g., auditors, inspectors general, evaluators, and certification agents). Commercial companies producing information technology products and systems, creating information security-related technologies, and providing information security services can also benefit from the information in this publication.

1.3 RELATIONSHIP TO OTHER SECURITY CONTROL PUBLICATIONS

To create the most technically sound and broadly applicable set of security controls for information systems, a variety of sources were considered during the development of this special publication. The sources included security controls from the defense, audit, financial, healthcare, and intelligence communities as well as controls defined by national and international standards organizations.[10] The objective of NIST Special Publication 800-53 is to provide a ~~sufficiently~~

[8] A federal information system is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

[9] NIST Special Publication 800-59 provides guidance on identifying an information system as a national security system.

[10] Security controls from the audit, defense, healthcare, intelligence, and standards communities are contained in the following publications: (i) Government Accountability Office, *Federal Information System Controls Audit Manual*; (ii) Department of Defense Instruction 8500.2, *Information Assurance Implementation*; (iii) Department of Health and Human Services Centers for Medicare and Medicaid Services, *Core Security Requirements*; (iv) Director of Central Intelligence Directive 6/3 Manual, *Protecting Sensitive Compartmented Information within Information Systems*; (v) NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*; and (vi) International Organization for Standardization/International Electrotechnical Commission 17799:2000, *Code of Practice for Information Security Management*.

~~rich~~ set of security controls that is sufficiently rich to satisfy the breadth and depth of security requirements[11] levied on information systems and that ~~are~~ is consistent with and complementary to other established security standards.

The catalog of security controls provided in Special Publication 800-53 can be effectively used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements. It is the responsibility of organizations to select the appropriate security controls,~~[12]~~ to implement the controls correctly, and to demonstrate the effectiveness of the controls in satisfying their stated security requirements. The security controls in the catalog facilitate the development of assessment methods and procedures that can be used to demonstrate control effectiveness in a consistent and repeatable manner—thus contributing to the organization's confidence that there is ongoing compliance with its stated security requirements.[13]

1.4 ORGANIZATIONAL RESPONSIBILITIES

Organizations should use FIPS 199 to define security categories for their information systems. This publication associates recommended minimum security controls with FIPS 199 low-impact, moderate-impact, and high-impact security categories. For each information system, ~~T~~the recommendation~~s~~ for minimum security controls from Special Publication 800-53 (i.e., the baseline security controls defined in Appendix D, tailored in accordance with the tailoring guidance in Section 3.3) ~~can subsequently~~ is intended to be used as a starting point for and input to the organization's risk assessment process.[14] The risk assessment ~~process refines~~ results are used to supplement the ~~initial set of minimum security controls with the~~ tailored baseline resulting in a set of agreed-upon controls documented in the security plan~~s~~ for ~~those~~ the information system~~s~~. While the FIPS 199 security categorization associates the operation of the information system with the potential impact on an organization's operations, ~~and~~ assets, or individuals, the incorporation of refined threat and vulnerability information during the risk assessment ~~process~~ facilitates ~~the tailoring~~ supplementing ~~of~~ the tailored baseline security controls to address organizational needs and tolerance for risk. ~~Deviations from the recommended baseline security controls should be made in accordance with the scoping guidance provided in this special publication and~~ The final, agreed-upon set of security controls should be documented with appropriate justification and supporting rationale in the security plan for the information system.

The use of security controls from Special Publication 800-53 and the incorporation of tailored baseline (minimum) controls as a starting point in the control selection process, facilitates a more consistent level of security ~~in an organizational~~ across federal information systems. It also offers

[11] Security requirements are those requirements levied on an information system that are derived from laws, Executive ~~o~~Orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

~~[12] NIST Special Publication 800-53 is the primary source of recommended security controls for federal information systems, replacing the security controls described in NIST Special Publications 800-18 and 800-26.~~

[13] NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), ~~spring~~ April 2006~~)~~, provides guidance on assessment methods and procedures for security controls defined in this publication. Special Publication 800-53A can also be used to conduct self-assessments of information systems.

[14] Risk assessments can be accomplished in a variety of ways depending on the specific needs of the organization. The assessment of risk is a process that should be incorporated into the system development life cycle, and the process should be reasonable for the organization concerned. NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance on the assessment and mitigation of risk as part of an overall risk management process.

the needed flexibility to ~~tailor~~ appropriately modify the controls based on specific organizational policy and requirements ~~documents~~, particular conditions and circumstances, known threat and vulnerability information, ~~or~~ and tolerance for risk to the organization's operations, ~~and~~ assets, or to individuals.

Building a more secure information system is a multifaceted undertaking that involves the use of: (i) well-defined system-level security requirements and security specifications; (ii) well-designed information technology component products; (iii) sound systems/security engineering principles and practices to effectively integrate component products into the information system; (iv) appropriate methods for product/system testing and evaluation; and (v) comprehensive system security planning and life cycle management.[15] From a systems engineering viewpoint, security is just one of many required capabilities for an organizational information system—capabilities that must be funded by the organization throughout the life cycle of the system. Realistically assessing the risks to an organization's operations and assets or to individuals by placing the information system into operation or continuing its operation is of utmost importance. Addressing the information system security requirements must be accomplished with full consideration of the risk tolerance of the organization ~~*and*~~ in light of the potential impacts, cost, schedule, and performance issues associated with the acquisition, deployment, and operation of the system.

1.5 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental concepts associated with security control selection and specification including: (i) the structural components of security controls and how the controls are organized into families; (ii) ~~the use of common security controls in support of organization-wide information security programs~~ minimum (baseline) security controls; (iii) ~~minimum security (baseline) controls~~ the use of common security controls in support of organization-wide information security programs; (iv) security controls in external environments; (~~i~~v) assurance in the effectiveness of security controls; and (vi) the commitment to maintain currency of the individual security controls and the control baselines.

- **Chapter Three** describes the process of selecting and specifying security controls for an information system including: (i) the organization's overall approach to managing risk; (ii) the security categorization of the system and the selection of minimum (baseline) security controls; (iii) the activities associated with tailoring the initial set of baseline security controls; ~~and~~ (iv) using ~~the~~ risk assessment results ~~potential for supplementing~~ to supplement the ~~initial~~ tailored security control baseline~~s~~, as necessary; and (v) how the organization applies risk management concepts in response to information system incidents.

- **Supporting appendices** provide more detailed security control selection and specification-related information including: (i) general references; (ii) definitions and terms; (iii) acronyms; (iv) minimum security controls for low-impact, moderate-impact, and high-impact information systems; (v) minimum assurance requirements; (vi) a master catalog of security controls; ~~and~~ (vii) mapping tables relating the security controls in this publication to other standards and control sets; (viii) crosswalks of NIST security standards and guidelines with

[15] Successful life cycle management depends on having qualified personnel to oversee and manage the information systems within an organization. The skills and knowledge of organizational personnel with information systems (and information security) responsibilities should be carefully evaluated (e.g., through performance, certification, etc.).

associated security controls; and (ix) guidance on the application of security controls to industrial control systems.

CHAPTER TWO

THE FUNDAMENTALS

SECURITY CONTROL STRUCTURE, ORGANIZATION, BASELINES, AND ASSURANCE

This chapter presents the fundamental concepts associated with security control selection and specification including: (i) the structure of security controls and the organization of the controls in the control catalog; (ii) the identification and use of common security controls; (iii) the application of minimum security controls, or control baselines, to information systems categorized in accordance with FIPS 199; (iv) security control assurance; and (v) future revisions to the security controls, the control catalog, and baseline controls.

2.1 SECURITY CONTROL ORGANIZATION AND STRUCTURE

Security controls in the security control catalog (Appendix F) have a well-defined organization and structure. The security controls are organized into *classes* and *families* for ease of use in the control selection and specification process. There are three general classes of security controls~~:~~ (i.e., management, operational, and technical) and seventeen security control families.[16] Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each control family. ~~Table~~ Figure 1 summarizes the classes and families in the security control catalog and the associated family identifiers.

~~CLASS~~	~~FAMILY~~	~~IDENTIFIER~~
~~Management~~	~~Risk Assessment~~	~~RA~~
~~Management~~	~~Planning~~	~~PL~~
~~Management~~	~~System and Services Acquisition~~	~~SA~~
~~Management~~	~~Certification, Accreditation, and Security Assessments~~	~~CA~~
~~Operational~~	~~Personnel Security~~	~~PS~~
~~Operational~~	~~Physical and Environmental Protection~~	~~PE~~
~~Operational~~	~~Contingency Planning~~	~~CP~~
~~Operational~~	~~Configuration Management~~	~~CM~~
~~Operational~~	~~Maintenance~~	~~MA~~
~~Operational~~	~~System and Information Integrity~~	~~SI~~
~~Operational~~	~~Media Protection~~	~~MP~~
~~Operational~~	~~Incident Response~~	~~IR~~
~~Operational~~	~~Awareness and Training~~	~~AT~~
~~Technical~~	~~Identification and Authentication~~	~~IA~~
~~Technical~~	~~Access Control~~	~~AC~~
~~Technical~~	~~Audit and Accountability~~	~~AU~~

[16] ~~Security control families in NIST Special Publication 800-53 are associated with one of three security control classes; (i.e., management, operational, technical).~~ The seventeen security control families in NIST Special Publication 800-53 are closely aligned with the seventeen security-related areas in FIPS 200 specifying the minimum security requirements for protecting federal information and information systems. Families are assigned to their respective classes based on the dominant characteristics of the controls in that family. Many security controls, however, can be logically associated with more than one class. For example, CP-1, the policy and procedures control from the Contingency Planning family, is listed as an operational control but also has characteristics that are consistent with security management as well.

~~Technical~~	~~System and Communications Protection~~	~~SC~~
IDENTIFIER	**FAMILY**	**CLASS**
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation, and Security Assessments	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

~~TABLE~~ FIGURE 1: SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS

To uniquely identify each control, a numeric identifier is appended to the family identifier to indicate the number of the control within the control family. For example, CP-9 is the ninth control in the Contingency Planning family.

The security control structure consists of three key components: (i) a *control* section; (ii) a *supplemental guidance* section; and (iii) a *control enhancements* section.[17] The following example from the ~~Contingency Planning~~ Auditing and Accountability family illustrates the structure of a typical security control.

~~CP-9 INFORMATION SYSTEM BACKUP~~

~~Control: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [*Assignment: organization-defined frequency*] and stores backup information an appropriately secured location.~~

~~Supplemental Guidance: The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives.~~

~~Control Enhancements:~~

~~(1) The organization tests backup information [*Assignment: organization-defined frequency*] to ensure media reliability and information integrity.~~

~~(2) The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.~~

~~(3) The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.~~

[17] A supplemental guidance section is also used for security control enhancements in situations where the guidance is not generally applicable to the entire control but instead focused on the particular control enhancement.

~~**(4) The organization encrypts backup information.**~~

~~**LOW** CP-9~~	~~**MOD** CP-9 (1)~~	~~**HIGH** CP-9 (1) (2) (3)~~

AU-2 AUDITABLE EVENTS

Control: The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*].

Supplemental Guidance: The purpose of auditing is to identify important events which are significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to intermittent problems. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents.

Control Enhancements:

(1) The information system provides the capability to compile audit records from multiple components throughout the system into a systemwide (logical or physical), time-correlated audit trail.

(2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.

(3) The organization periodically reviews and updates the list of organization-defined auditable events.

LOW AU-2	**MOD** AU-2 (3)	**HIGH** AU-2 (1) (2) (3)

The control section provides a concise statement of the specific security capability needed to protect a particular aspect of an information system. The control statement describes specific security-related activities or actions to be carried out by the organization or by the information system. For some controls in the control catalog, a degree of flexibility is provided by allowing organizations to selectively define input values for certain parameters associated with the controls. This flexibility is achieved through the use of *assignment* and *selection* operations within the main body of the control. Assignment and selection operations provide an opportunity for an organization to tailor the security controls to support specific mission, business, or operational needs. For example, an organization can specify ~~how often it intends to conduct information system backups or how frequently it intends to test its contingency plan~~ the specific events to be audited. Once specified, the organization-defined value becomes part of the control, and the organization is assessed against the completed control statement. Some assignment operations may specify minimum or maximum values that constrain the values that may be input by the organization. Selection statements also narrow the potential input values by providing a specific list of items from which the organization must choose.

The supplemental guidance section provides additional information related to a specific security control. Organizations should consider supplemental guidance when defining, developing, and implementing security controls. Applicable federal legislation, Executive Orders, directives, policies, regulations, standards, and guidance documents (e.g., OMB Circulars, FIPS, and NIST Special Publications) are listed in the supplemental guidance section, when appropriate, for the particular security control.

The control enhancements section provides statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control. In both cases, the control enhancements are used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additions to a basic control's functionality based on the results of a risk assessment. Control enhancements are numbered sequentially within each control so that the enhancements can be easily identified when selected to supplement the basic control. In the example above, if all three ~~two of the three~~ control enhancements are selected, the control designation subsequently becomes ~~CP-9 (1) (2)~~ AU-2 (1) (2) (3). The numerical designation of a security control enhancement is used only to identify a particular enhancement within the control structure. The designation is neither indicative of the relative strength of the control enhancement nor assumes any hierarchical relationship among enhancements. In the above example, enhancement (3) is used before (1) and (2) since that enhancement is appropriate at a lower level than the other two. This type of situation arises from the decision to enhance control stability in the face of change by not renumbering existing enhancements when new ones are added or when decisions about placement within baselines changes.

2.2 SECURITY CONTROL BASELINES

Organizations ~~must~~ are required to employ security controls to meet security requirements defined by laws, Executive Orders, directives, policies, or regulations (e.g., Federal Information Security Management Act, OMB Circular A-130, Appendix III).[18] The challenge for organizations is to determine the appropriate set of security controls, which if implemented and determined to be effective in their application, would most cost-effectively comply with the stated security requirements. Selecting the appropriate set of security controls to meet the specific, and sometimes unique, security requirements of an organization is an important task—a task that demonstrates the organization's commitment to security and the due diligence exercised in protecting the confidentiality, integrity, and availability of their information and information systems.

To assist organizations in making the appropriate selection of security controls for their information systems, the concept of *baseline* controls is introduced. Baseline controls are the minimum security controls recommended for an information system based on the system's security categorization in accordance with FIPS 199.[19] ~~Security categories derived from FIPS 199 are typically considered during the risk assessment process to help guide the initial selection of security controls for an information system.[20] The risk assessment process provides useful information and a procedural approach to examining the important factors that ultimately determine which security controls are necessary to protect the organization's operations and assets.~~ The tailored security control baseline ~~controls associated with the FIPS 199 security~~

[18] An information system may require security controls at different layers within the system. For example, an operating system or network component typically provides an identification and authentication capability. An application running on that operating system or network may also provide its own identification and authentication capability rendering an additional level of protection for the overall information system. The selection and specification of security controls should consider components at all layers within the information system.

[19] FIPS 199 security categories are based on the potential impact on an organization or individuals should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

~~[20] Security categories are used in conjunction with vulnerability and threat information in assessing the risk to an organization by operating an information system. FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions takes place within the context of each organization and the overall national interest.~~

~~categories~~ (i.e., the appropriate control baseline from Appendix D tailored in accordance with the guidance in Section 3.3) serves as ~~a~~ the *starting point* for organizations in determining the appropriate safeguards and countermeasures necessary to protect their information systems. Because the baselines are intended to be broadly applicable starting points, ~~modifications~~ supplements to the ~~selected~~ tailored baselines (see Section 3.4) ~~may~~ will likely be necessary in order to achieve adequate risk mitigation. ~~Such modifications~~ The tailored baselines are ~~tied to the~~ supplemented based on organizational assessments of risk ~~assessment~~ and the resulting controls documented in the security plans for the information systems.

Appendix D provides a listing of minimum security controls. Three sets of minimum security (baseline) controls have been identified corresponding to the low-impact, moderate-impact, and high-impact levels defined in the security categorization process in FIPS 199 and derived in Section 3.2 below. Each of the three baselines provides a minimum set of security controls (or floor) for a particular impact level associated with a security category. Appendix F provides the complete catalog of security controls for information systems, arranged by control families. The catalog represents the entire set of security controls defined at this time. Chapter 3 provides additional information on how to use security categories to select the appropriate set of baseline security controls, how to apply the tailoring guidance to the baseline controls, and how to supplement the tailored baseline in order to achieve adequate risk mitigation.

Implementation Tip

Since the baseline security controls represent the minimum controls for low-impact, moderate-impact, and high-impact information systems, respectively, there are additional controls and control enhancements that appear in the catalog that are not used in any of the baselines. These additional security controls and control enhancements for the information system are available to organizations and can be used in supplementing the tailored baselines to achieve the needed level of protection in accordance with an organizational assessment of risk. Moreover, security controls and control enhancements contained in higher-level baselines can also be used by organizations to strengthen the level of protection provided in lower-level baselines, if deemed appropriate. At the end of the security control selection and specification process, the agreed-upon set of security controls documented in the security plan, must be sufficient to provide adequate security for the organization and mitigate risks to its operations, assets, and individuals.

2.3 COMMON SECURITY CONTROLS

An organization-wide view of an information security program facilitates the identification of *common security controls* that can be applied to one or more organizational information systems. Common security controls can apply to: (i) all organizational information systems; (ii) a group of information systems at a specific site; or (iii) common information systems, subsystems, or applications (i.e., common hardware, software, and/or firmware) deployed at multiple operational sites. Common security controls have the following properties:

- The development, implementation, and assessment of common security controls can be assigned to responsible organizational officials or organizational elements (other than the information system owners whose systems will implement or use the common security controls); and
- The results from the assessment of the common security controls can be used to support the security certification and accreditation processes of organizational information systems where the controls have been applied.[21]

[21] NIST Special Publication 800-37 provides guidance on security certification and accreditation of information systems.

The identification of common security controls is most effectively accomplished as an organization-wide exercise with the involvement of the chief information officer, senior agency information security officer, authorizing officials, information system owners/program managers, information owners, and information system security officers. The organization-wide exercise considers the ~~classes~~ categories of information systems within the organization in accordance with FIPS 199 (i.e., low-impact, moderate-impact, or high-impact information systems) and the minimum security controls necessary to protect the operations and assets supported by those systems (see *baseline* security controls in Section 2.2). For example, common security controls can be identified for all low-impact information systems by considering the baseline security controls for that ~~class~~ category of information system. Similar exercises can be conducted for moderate-impact and high-impact systems as well.

Many of the security controls needed to protect an information system (e.g., contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls) may be excellent candidates for common security control status. By centrally managing the development, implementation, and assessment of the common security controls designated by the organization, security costs can be amortized across multiple information systems. Security controls not designated as common controls are considered *system-specific controls* and are the responsibility of the information system owner. Security plans for individual information systems should clearly identify which security controls have been designated by the organization as common security controls and which controls have been designated as system-specific controls.

Organizations may also assign a *hybrid* status to security controls in situations where one part of the control is deemed to be common, while another part of the control is deemed to be system-specific. For example, an organization may view the IR-1 (Incident Response Policy and Procedures) security control as a hybrid control with the policy portion of the control deemed to be common and the procedures portion of the control deemed to be system-specific. Hybrid security controls may also serve as templates for further control refinement. An organization may choose, for example, to implement the CP-2 (Contingency Planning) security control as a master template for a generalized contingency plan for all organizational information systems with individual information system owners tailoring the plan, where appropriate, for system-specific issues.

Information system owners are responsible for any system-specific issues associated with the implementation of an organization's common security controls. These issues are identified and described in the system security plans for the individual information systems. The senior agency information security officer, acting on behalf of the chief information officer, should coordinate with organizational officials (e.g., facilities managers, site managers, personnel managers) responsible for the development and implementation of the designated common security controls to ensure that the required controls are put into place, the controls are assessed, and the assessment results are shared with the appropriate information system owners to better support the security accreditation process.

Partitioning security controls into common ~~security~~ controls and system-specific ~~security~~ controls can result in significant savings to the organization in ~~control~~ development and implementation costs especially when the common controls serve multiple information systems and entities. It can also result in a more consistent application of the security controls across the organization at large. Moreover, equally significant savings can be realized in the security certification and accreditation process. Rather than assessing common security controls in every information system, the certification process draws upon any applicable results from the most current assessment of the common security controls performed at the organization level. An organization-wide approach to reuse and sharing of assessment results can greatly enhance the efficiency of the security certifications and accreditations being conducted by organizations and significantly reduce security program costs.

While the concept of security control partitioning into common security controls and system-specific controls is straightforward and intuitive, the application of this principle within an organization takes planning, coordination, and perseverance. If an organization is just beginning to implement this approach or has only partially implemented this approach, it may take some time to get the maximum benefits from security control partitioning and the associated reuse of assessment evidence. Because of the potential dependence on common security controls by many of an organization's information systems, a failure of such common controls may result in a significant increase in agency-level risk—risk that arises from the operation of the systems that depend on these controls.

Implementation Tip

The FIPS 199 security categorization process and the selection of common security controls are closely related activities that are most effectively accomplished on an organization-wide basis with the involvement of the organization's senior leadership (i.e., authorizing officials, chief information officer, senior agency information security officer, information system owners, and mission/information owners). These individuals have the collective corporate knowledge to understand the organization's priorities, the importance of the organization's operations (including mission, functions, image, and reputation) and assets, and the relative importance of the organizational information systems that support those operations and assets. The organization's senior leaders are also in the best position to select the common security controls for each of the security control baselines and assign organizational responsibilities for developing, implementing, and assessing those controls.

2.4 SECURITY CONTROLS IN EXTERNAL ENVIRONMENTS

Organizations are becoming increasingly reliant on external service providers to carry out important missions and functions. Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements), licensing agreements, and/or supply chain exchanges. The growing dependence on external service providers and new relationships being forged with business partners[22] presents new and difficult challenges for the organization, especially in the area of information security. These challenges include: (i) defining the types of services provided to the organization by external entities; (ii) describing how the provided services are protected in accordance with the security requirements of the organization; and (iii) obtaining the necessary assurances that the risk to the organization's operations, assets, and individuals arising from the provision of services by external entities is at an acceptable level.

The responsibility for information security remains with the organization and cannot be transferred to third parties. Organizations must establish an appropriate *chain of trust* for information security when dealing with external service providers. The chain of trust ensures that the security controls required for the protection of information systems supporting the

[22] Business partners may either be trusted (e.g., supplier-manufacturer relationship) or untrusted (e.g., competitors in a market sector). Information exchanges may be required among cooperative business partners. The risk of exchanging information among business partners and other external entities must be assessed and appropriate security controls employed. There may be laws, regulations, or contracts that protect this information from unauthorized disclosure.

organization are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the organization. Trust is generally established by assessment of the products, systems, organizations, and individuals providing the essential security controls. A chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization.

The chain of trust can be very complicated due to the number of entities participating in the consumer-provider relationship and the type of relationship between the parties. A service provider provides its services to an organization or may offer those services on behalf of an organization. The organization (i.e., "consuming party" in the relationship) is justified in expecting that one aspect of the provided service will be the provision of appropriate information security services including associated security controls. Security, in this case, becomes part of the contract between the consuming organization and the service provider. However, even when there is a contractual relationship between the organization and the service provider, the nature of that contract may not be such that it provides the basis for the necessary level of trust. Depending on the nature of the service, it may simply be unwise for the organization to wholly trust the provider—not due to any inherent untrustworthiness on the provider's part, but due to the intrinsic level of risk in the service. Contracts between the organization and external service providers may also require the active participation of the organization. For example, the organization may be required by the contract to install public key encryption-enabled client software recommended by the service provider. External service providers may also in turn outsource the services to other external entities, making the chain of trust even more complicated and difficult to manage.

Security controls provided by external service providers have many of the same characteristics of the common security controls designated by the organization including:

- The development, implementation, and assessment of the security controls can be assigned to responsible entities external to the organization that provide information system services to the organization; and
- The results from the assessments of the security controls employed by external service providers can be used to support the security certification and accreditation processes of information systems within organizations that rely on these services.

In reality, the provision of services by external providers may result in some services without explicit agreements between the organization and the external entities responsible for the services. Whenever explicit agreements are feasible (e.g., through contracts, service level agreements, etc.), the organization should develop such agreements and use the security controls in Special Publication 800-53 including the controls associated with outsourced services. When the organization is not in a position to require explicit agreements with service providers (e.g., when the service is imposed on the organization or when the service is a commercial commodity), the organization should establish explicit assumptions about the service capabilities with regard to security. These assumptions should be based upon reasonable expectations toward the service, both what is practical and what is actually available. The assumptions should also be made known to the organization requiring use of the service and, as feasible, to the service provider.

Organizations should carefully assess the prospective services offered by entities outside of the organization to determine the necessary security requirements for those services. Organizations should also determine the appropriate mix of security controls (i.e., common, hybrid, and system-specific) and ensure that the participating parties in joint ventures, business partnerships, outsourcing arrangements, licensing agreements or any other relationship resulting in the use of information system services from external service providers are assigned and aware of their responsibilities for developing, implementing, and assessing the required security controls. It is highly recommended that organizations, either through their own personnel or through external contractors, have the contractual right to assess and verify that external service providers are, in fact, implementing appropriate information security controls as required by the service agreements. Authorizing officials must have confidence in the overall security of their information systems to include the services provided by external entities.

2.5 SECURITY CONTROL ASSURANCE

Assurance is the grounds for confidence that the security controls implemented within an information system are effective in their application. Assurance can be obtained in a variety of ways including: (i) actions taken by developers and implementers of security controls ~~to use state-of-the-practice~~ in the design, development, and implementation techniques and methods; and (ii) actions taken by security control assessors during the testing and evaluation process to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Assurance considerations related to developers and implementers of security controls are addressed in this special publication. Assurance considerations related to assessors of security controls (including certification agents, evaluators, auditors, inspectors general) are addressed in NIST Special Publication 800-53A.~~[23]~~

Appendix E describes the minimum assurance requirements for security controls listed in the low, moderate, and high baselines. For security controls in the low baseline, the emphasis is on the control being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner. For security controls in the moderate baseline, the emphasis is on ensuring control correctness. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer or control implementer incorporates, as part of the control, specific capabilities to ensure that the control meets its function or purpose. For security controls in the high baseline, the emphasis is on requiring within the control, the capabilities that are needed to support ongoing, consistent operation of the control and to support continuous improvement in the control's effectiveness. There are additional assurance requirements available to developers and implementers supplementing the minimum assurance requirements for the high baseline in order to protect against threats from highly skilled, highly motivated, and well-financed threat agents. This level of protection is ~~required~~ necessary for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above.

2.6 REVISIONS AND EXTENSIONS

The set of security controls listed in the control catalog represents the current state-of-the-practice safeguards and countermeasures for information systems. The security controls will be reviewed and revised ~~and extended~~ periodically[24] to reflect: (i) the experience gained from using the

~~[23] NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), is projected for publication in the spring 2006.~~

[24] Currently, NIST plans to review and revise the security control catalog and security control baselines in Special Publication 800-53 on a biennial basis. The proposed modifications to security controls and security control baselines will be carefully weighed with each revision cycle considering the desire for stability on one hand, and the need to respond to changing threats and vulnerabilities, new attack methods, new technologies, and the important objective of raising the foundational level of security over time.

controls; (ii) the changing security requirements within organizations; (iii) emerging threats and attack methods; and (~~ii~~iv) the availability of new security technologies ~~that may be available~~. The controls ~~populating the various families~~ in the control catalog are expected to change over time, as controls are eliminated or revised and new controls are added. ~~The proposed additions, deletions, or modifications to the catalog of security controls will go through a rigorous, public review process to obtain government and private sector feedback and to build consensus for the changes.~~ The minimum security controls defined in the low, moderate, and high baselines are also expected to change over time ~~as well,~~ as the level of security and due diligence for mitigating risks within organizations increases. In addition to the need for change, the need for stability will be addressed by requiring that proposed additions, deletions, or modifications to the catalog of security controls go through a rigorous, public review process to obtain government and private sector feedback and to build consensus for the changes. A ~~dynamic~~ stable, yet flexible and technically rigorous set of security controls will be maintained in the control catalog ~~to allow organizations and communities of interest to continue to be able to select the appropriate controls for their respective needs in a cost-effective manner~~.

CHAPTER THREE

THE PROCESS

SELECTION AND SPECIFICATION OF SECURITY CONTROLS

This chapter describes the process of selecting and specifying security controls for an information system including: (i) the organization's overall approach to managing risk; (ii) the security categorization of the system in accordance with FIPS 199 and the selection of minimum (baseline) security controls; (iii) the activities associated with tailoring the initial set of baseline security controls through the application of ~~scoping~~ tailoring guidance;[25] ~~and the assignment of organization-defined parameters; and~~ (iv) ~~the potential for supplementing the minimum security controls with additional controls, as necessary, to achieve adequate security~~ applying the results from the risk assessment process to supplement, as necessary, the tailored security control baseline; and (v) how the organization applies risk management concepts in response to information system incidents.

3.1 MANAGING ORGANIZATIONAL RISK

The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program that involves the management of organizational risk—that is, the risk to the organization or to individuals associated with the operation of an information system. The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system—the security controls necessary to protect individuals and the operations and assets of the organization. ~~Managing organizational risk includes several important activities: (i) assessing risk; (ii) conducting cost-benefit analyses; (iii) selecting, implementing, and assessing security controls; and (iv) formally authorizing the information system for operation (also known as security accreditation).~~ The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations. The following activities related to managing organizational risk (also known as the NIST Risk Framework) are paramount to an effective information security program and can be applied to both new and legacy information systems within the context of the system development life cycle and the Federal Enterprise Architecture—

- ***Categorize*** the information system and the information resident within that system based on a FIPS 199 impact analysis.

- ***Select*** an initial set of security controls (i.e., baseline from Appendix D) for the information system ~~as a starting point~~ based on the FIPS 199 security categorization and apply tailoring guidance from Section 3.3 as appropriate, to obtain a starting point for required controls.

- ~~***Adjust***~~ ~~(or tailor)~~ ***Supplement*** the initial set of tailored security controls based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, ~~the availability of compensating controls,~~ or special circumstances.[26]

[25] ~~Scoping~~ Tailoring guidance provides organizations with specific considerations on the applicability and implementation of individual security controls in the control baselines (~~s~~See Section 3.3).

[26] NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance on the assessment and mitigation of risk.

- ***Document*** the agreed-upon set of security controls in the system security plan including the organization's justification for any refinements or adjustments to the initial set of controls.[27]
- ***Implement*** the security controls in the information system. For legacy systems, some or all of the security controls selected may already be in place.
- ***Assess*** the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.[28]
- ***Determine*** the risk to organizational operations, ~~and~~ organizational assets, or individuals resulting from the ~~planned or continued~~ operation of the information system.
- ***Authorize*** information system ~~processing~~ operation (or for legacy systems, authorize continued system ~~processing~~ operation) if the ~~level of~~ risk to ~~the organization's~~ organizational operations, ~~or~~ organizational assets, or individuals is acceptable.[29]
- ***Monitor*** and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis.

The remainder of this chapter focuses on the first three activities in managing organizational risk—the FIPS 199 security categorization, the initial selection and tailoring of security controls based on the security categorization, and ~~the tailoring of~~ supplementing the initial controls based on the organization's risk assessment.

3.2 SECURITY CATEGORIZATION AND BASELINE SELECTION

FIPS 199, the mandatory federal security categorization standard, is predicated on a simple and well-established concept—determining appropriate priorities for organizational information systems and subsequently applying appropriate measures to adequately protect those systems. The security controls applied to a particular information system should be commensurate with the potential impact on organizational operations, organizational assets, or individuals should there be a ~~breach in security due to the~~ loss of confidentiality, integrity, or availability. FIPS 199 requires organizations to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values assigned to the respective security objectives are the highest values (i.e., high water mark) from among the security categories that have been determined for each type of information resident on those information systems.[30] The generalized format for expressing the security category (SC) of an information system is:

$$\textbf{SC}_{\text{information system}} = \{(\textbf{confidentiality}, \textit{impact}), (\textbf{integrity}, \textit{impact}), (\textbf{availability}, \textit{impact})\},$$

[27] NIST Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, provides guidance on documenting information system security controls.

[28] NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), ~~projected for publication in the spring~~ April 2006~~)~~, provides guidance for determining the effectiveness of security controls.

[29] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides guidance on the security authorization of information systems.

[30] NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, provides guidance on the assignment of security categories to information systems.

where the acceptable values for potential impact are low, moderate, or high.

Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept is used to determine the impact level of the information system for the express purpose of selecting an initial set of security controls from one of the three security control baselines.[31] Thus, a *low-impact* system is defined as an information system in which all three of the security objectives are low. A *moderate-impact* system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a *high-impact* system is an information system in which at least one security objective is high. Once the overall impact level of the information system is determined, an initial set of security controls can be selected from the corresponding low, moderate, or high baselines listed in Appendix D.

Implementation Tip

To determine the overall impact level of the information system, first determine the different types of information that are processed, stored, or transmitted by the information system (e.g., financial sector oversight, inspections and auditing, official information dissemination, etc.). NIST Special Publication 800-60 provides guidance on a variety of information types commonly used by organizations. Second, using the impact levels in FIPS 199, categorize the confidentiality, integrity, and availability of each information type as low, moderate, or high. Third, determine the highest impact level for each information type (i.e., the high water mark for each information type). Fourth, determine the highest impact level from all information types resident on the information system (i.e., the high water mark for the information system). The result is the overall impact level of the information system.

3.3 TAILORING THE INITIAL BASELINE

Organizations have the flexibility to tailor the security control baselines in accordance with the terms and conditions set forth in this publication. Tailoring activities include: (i) the application of appropriate *scoping guidance* to the initial baseline; (ii) the specification of *compensating security controls*, if needed; ~~(iii) the specification of *additional security controls*, when required;~~ and (iii~~v~~) the specification of *organization-defined parameters* in the security controls, where allowed. To ensure a cost-effective, risk-based approach to achieving adequate information security organization-wide, security control baseline tailoring activities should be coordinated with and approved by appropriate organizational officials (e.g., chief information officers, senior agency information security officers, authorizing officials, or authorizing officials' designated representatives). ~~The resulting set of security controls is documented in the security plan for the information system.[32]~~

[31] The high water mark concept is employed because there are significant dependencies among the security objectives of confidentiality, integrity, and availability. In most cases, a compromise in one security objective ultimately affects the other security objectives as well. Accordingly, the security controls in the control catalog are not categorized by security objective—rather, they are grouped into baselines to provide a general protection capability for classes of information systems based on impact level. The application of scoping guidance may allow selective security control baseline ~~adjustments or~~ tailoring (See Section 3.3).

~~[32] It is important for organizations to document the decisions taken during the security control process providing a sound rationale and justification for those decisions whenever possible. This documentation is essential when examining the overall security considerations for information systems with respect to potential mission and/or business case impact.~~

Scoping Guidance

Scoping guidance provides organizations with specific terms and conditions on the applicability and implementation of individual security controls in the security control baselines. There are several considerations, described below, that can potentially impact how the baseline security controls are applied by the organization:

Operational/environmental-related considerations—

- Security controls that are dependent on the nature of the operational environment are applicable only if the information system is employed in an environment necessitating the controls. For example, certain physical security controls may not be applicable to space-based information systems, and temperature and humidity controls may not be applicable to remote sensors that exist outside of the indoor facilities that contain information systems.

Technology-related considerations—

- Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) are applicable only if those technologies are employed or are required to be employed within the information system.

- Security controls are applicable only to the components of the information system that provide or support the security capability addressed by the control.[33] For example, when information system components ~~that~~ are single-user, not networked, or only locally networked, one or more of these characteristics may provide appropriate rationale for not applying selected controls to that component.

- Security controls that can be either explicitly or implicitly supported by automated mechanisms, do not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products. In situations where automated mechanisms are not readily available, cost-effective, or technically feasible, compensating security controls, implemented through nonautomated mechanisms or procedures, ~~may~~ should be used to satisfy specified security controls or control enhancements (see terms and conditions for applying compensating controls below).

Scalability-related considerations—

- Security controls are scalable ~~either by the size of the particular organization implementing the controls or~~ with regard to the extent and rigor of the control implementation. Scalability is guided by the FIPS 199 security categorization of the information system being protected. ~~or both~~ ~~The following examples take both scalability factors into consideration. A~~ For example, a contingency plan for a ~~large organization with a~~ FIPS 199 ~~moderate-impact or~~ high-impact information system may be quite lengthy and contain a significant amount of implementation detail. In contrast, a contingency plan for ~~a smaller organization with~~ a FIPS

[33] For example, auditing controls would typically be applied to the components of an information system that provide or should provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the organization. Organizations should carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an organizational assessment of risk. While the tailoring guidance may support not applying a particular security control to a specific component (e.g., the audit example above), any residual risks associated with the absence of that control must still be addressed and mitigated as necessary, to adequately protect the organization's operations, assets, and individuals.

199 low-impact information system may be considerably shorter and contain much less implementation detail. Organizations should use discretion in ~~scaling~~ applying the security controls to information systems, giving consideration to the scalability factors in ~~the~~ particular environments. ~~of use~~ ~~to ensure~~ This approach facilitates a cost-effective, risk-based approach to security control implementation that expends no more resources than necessary, yet achieves sufficient risk mitigation and adequate security.

Physical Infrastructure-related considerations—

- Security controls that refer to organizational facilities (e.g., physical controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) are applicable only to those sections of the facilities that directly provide protection to, support for, or are related to the information system (including its information technology assets such as electronic mail or web servers, server farms, data centers, networking nodes, controlled interface equipment, and communications equipment).

~~Risk~~Security objective-related considerations—

- Security controls that uniquely support the confidentiality, integrity, or availability security objectives may be downgraded to the corresponding control in a lower baseline (or appropriately modified or eliminated if not defined in a lower baseline) if, and only if, the downgrading action: (i) is consistent with the FIPS 199 security categorization for the corresponding security objectives of confidentiality, integrity, or availability before moving to the high water mark;[34] (ii) is supported by an organizational assessment of risk; and (iii) does not affect the security-relevant information within the information system.[35] The following security controls are recommended candidates for downgrading: (i) ~~for~~ confidentiality [AC-15, MA-3 (3), MP-3, MP-6, PE-5, SC-4, SC-9]; (ii) ~~for~~ integrity [SC-8]; and (iii) ~~for~~ availability [CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, MA-6, PE-9, PE-10, PE-13, PE-15, SC-6].[36]

[34] When applying the "high water mark" process in Section 3.2, some of the original FIPS 199 confidentiality, integrity, or availability security objectives may have been upgraded to a higher baseline of security controls. As part of this process, security controls that uniquely support the confidentiality, integrity, or availability security objectives may have been upgraded unnecessarily. Consequently, it is recommended that organizations consider appropriate and allowable downgrading actions to ensure cost-effective, risk-based application of security controls.

[35] Information that is security-relevant at the system level (e.g., password files, network routing tables, cryptographic key management information) is distinguished from user-level information within an information system. Certain security controls within an information system are used to support the security objectives of confidentiality and integrity for both user-level and system-level information. Caution should be exercised in downgrading confidentiality or integrity-related security controls to ensure that the downgrading action does not ~~affect~~ result in insufficient protection for the security-relevant information within the information system. Security-relevant information must be protected at the high water mark in order to achieve that level of protection for any of the security objectives related to user-level information.

[36] Certain security controls that are uniquely attributable to confidentiality, integrity, or availability that would ordinarily be considered as potential candidates for downgrading (e.g., AC-16, AU-10, CP-5, IA-7, MP-6, PE-12, PE-14, PL-5, SC-5, SC-13, SC-14, SC-16) are eliminated from consideration because the controls are either selected for use in all baselines and have no enhancements that could be downgraded, or the controls are optional and not selected for use in any baseline. Organizations should exercise extreme caution when considering downgrading actions on any security controls that do not appear in the list in Section 3.3 to ensure that the downgrading action does not affect security objectives other than the objectives targeted for downgrading.

Public access-related considerations—

- Security controls associated with public access information systems should be carefully considered and applied with discretion since some security controls from the specified control baselines (e.g., identification and authentication, personnel security controls) may not be applicable to users accessing information systems through public interfaces. For example, while the baseline controls require identification and authentication of ~~agency~~ organizational personnel that maintain and support information systems providing the public access services, the same controls might not be required for ~~users accessing~~ access to those information systems through public interfaces to obtain publicly available information. On the other hand, identification and authentication would be required for users accessing information systems through public interfaces in some instances, for example, to access/change their ~~private/~~personal information.

Policy/regulatory-related considerations—

Security controls that address matters governed by federal laws, directives, policies, or regulations (e.g., privacy impact assessments) are required only if the employment of those controls is consistent with the types of information and information systems covered by the applicable laws, directives, policies, or regulations.

Common security control-related considerations—

- Security controls designated by the organization as common controls are, in most cases, managed by an organizational entity other than the information system owner. Organizational decisions on which security controls are viewed as common controls may greatly affect the responsibilities of individual information system owners with regard to the implementation of controls in a particular baseline. ~~Decisions on common control designations should not, however, affect the organization's responsibility to provide the security controls included in the baseline.~~ Every control in a baseline must be fully addressed either by the organization or the information system owner.

Compensating Security Controls

With the diverse nature of today's information systems, organizations may find it necessary, on occasion, to specify and employ compensating security controls. A compensating security control is a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines described in NIST Special Publication 800-53, which provides equivalent or comparable protection for an information system.[37] A compensating control for an information system may be employed by an organization only under the following conditions: (i) the organization selects the compensating control from NIST Special Publication 800-53, or if an appropriate compensating control is not available in the security control catalog, the organization adopts a suitable compensating control;[38] (ii) the organization provides a complete and

[37] More than one compensating control may be required to provide the equivalent or comparable protection for a particular security control in NIST Special Publication 800-53. For example, an organization with significant staff limitations may have difficulty in meeting the separation of duty security control but may employ compensating controls by strengthening the audit and accountability controls and personnel security controls within the information system.

[38] Organizations should make every attempt to select compensating controls from the security control catalog in NIST Special Publication 800-53. Organization-defined compensating controls should be used only as a last resort when the security control catalog does not contain suitable compensating controls.

convincing rationale and justification[39] for how the compensating control provides an equivalent security capability or level of protection for the information system and why the related baseline security control could not be employed; and (iii) the organization assesses and formally accepts the risk associated with employing the compensating control in the information system. The use of compensating security controls should be ~~reviewed,~~ documented in the system security plan~~,~~ and approved by the authorizing official for the information system.

Organization-Defined Security Control Parameters

Security controls containing organization-defined parameters (i.e., assignment and/or selection operations) give organizations the flexibility to define selected portions of the controls to support specific organizational requirements or objectives (see AU-2 example in Section 2.1). After the application of the scoping guidance~~,~~ and the selection of compensating security controls, organizations should review the list of security controls for assignment and selection operations and provide appropriate organization-defined values for the identified parameters. Where specified, minimum and maximum values for organization-defined parameters should be adhered to unless more restrictive values are prescribed by applicable laws, directives, Executive Orders, policies, standards, or regulations or are indicated by the risk assessment in order to adequately mitigate risk.

3.4 SUPPLEMENTING THE TAILORED BASELINE

The tailored security control baseline~~s~~ ~~listed in Appendix D~~ should be viewed as the foundation~~s~~ or starting point~~s~~ in the selection of adequate security controls for an information system. The tailored baseline~~s~~ represents, for a particular class~~es~~ of information system~~s~~ (derived from the FIPS 199 security categorization~~s~~ and modified appropriately for local conditions), the ~~minimum~~ starting point for determining the needed level of security *due diligence* to be demonstrated by an organization toward the protection of its operations and assets. As described in Section 3.1, the final determination of the appropriate set of security controls necessary to provide adequate security for an information system is a function of the organization's assessment of risk and what is required to sufficiently mitigate the risks to organizational operations, organizational assets, or individuals.

In many cases, additional ~~or enhanced~~ security controls or control enhancements will be needed to address specific threats to and vulnerabilities in an information system or to satisfy the requirements of applicable laws, directives, Executive Orders, policies, standards, or regulations. The risk assessment at this stage in the security control selection process provides important inputs to determine the sufficiency of the security controls in the tailored baseline—that is, the security controls needed to adequately protect the organization's operations (including mission, function, image, and reputation), the organization's assets, and individuals. Organizations are encouraged to make maximum use of the security control catalog to facilitate the process of enhancing security controls or adding controls to the ~~current~~ tailored baseline~~s~~. To assist in this process, numerous controls and control enhancements are available in the security control catalog that are found in only higher-impact baselines or are not included in any of the baselines. ~~The techniques and methodologies used by organizations in supplementing the security control baselines are beyond the scope of this special publication.~~

[39] The depth and rigor of the rationale and justification provided should be scaled to the FIPS 199 impact level of the information system, with significantly less explanation needed for a low-impact system than for a high-impact system.

The resulting set of agreed-upon security controls along with the supporting rationale and justification for control selection decisions are documented in the security plan for the information system.[40] Figure 2 summarizes the security control selection process, including the tailoring of the initial security control baseline and any additional modifications to the baseline required based on the organization's assessment of risk.

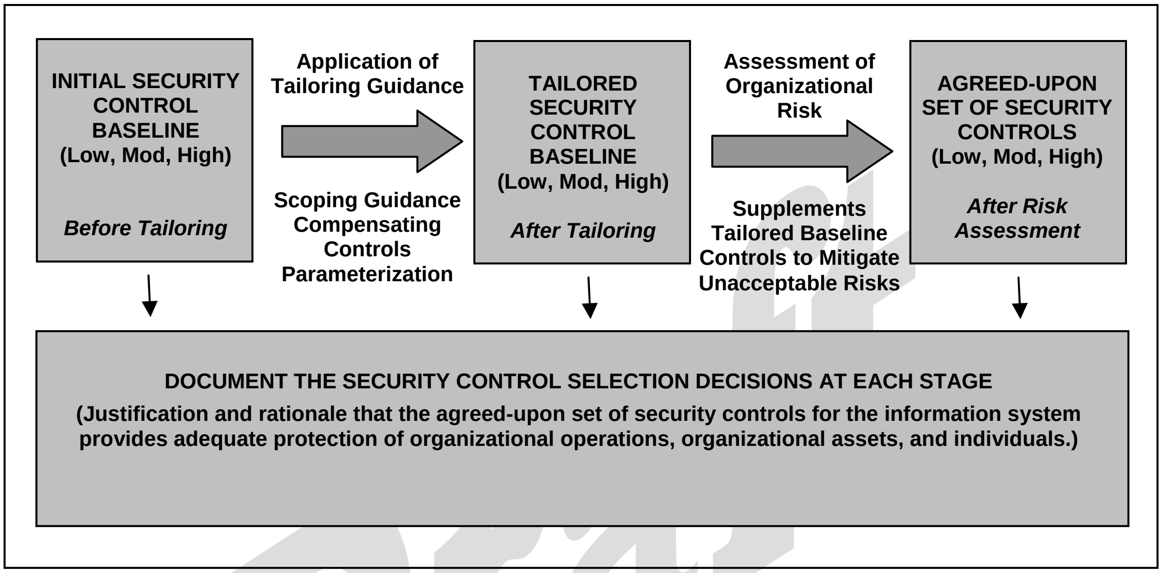
INITIAL SECURITY CONTROL BASELINE (Low, Mod, High)
Before Tailoring
Application of Tailoring Guidance
Scoping Guidance
Compensating Controls
Parameterization
TAILORED SECURITY CONTROL BASELINE (Low, Mod, High)
After Tailoring
Assessment of Organizational Risk
Supplements Tailored Baseline Controls to Mitigate Unacceptable Risks
AGREED-UPON SET OF SECURITY CONTROLS (Low, Mod, High)
After Risk Assessment
DOCUMENT THE SECURITY CONTROL SELECTION DECISIONS AT EACH STAGE
(Justification and rationale that the agreed-upon set of security controls for the information system provides adequate protection of organizational operations, organizational assets, and individuals.)

FIGURE 2: SECURITY CONTROL SELECTION PROCESS

[40] It is important for organizations to document the decisions taken during the security control ~~baseline tailoring~~ selection process providing a sound rationale and justification for those decisions whenever possible. This documentation is essential when examining the overall security considerations for information systems with respect to potential mission and/or business case impact.

3.5 RESPONDING TO INFORMATION SYSTEM INCIDENTS

Organizations should initiate specific actions as part of a comprehensive incident response process when a security-related incident occurs on an organizational information system.[41] Specifically, the organization should revisit the risk management activities described in the risk framework in Section 3.1. As important elements of the incident response process, organizations should at a minimum:

- Reconfirm the criticality/sensitivity of the information system and the information processed, stored, and/or transmitted by that system.

  The organization should reexamine the FIPS 199 impact level of the information system to confirm the criticality/sensitivity of the system in supporting its mission operations or business case. The resulting impact on organizational operations, organizational assets, or individuals resulting from the incident may provide new insights as to the overall importance of the system in allowing the organization to fulfill its mission responsibilities.

- Assess the current security state of the information system after the incident and reassess the current risk to organizational operations, organizational assets, and individuals.

  The organization should investigate the information system vulnerability (or vulnerabilities) exploited by the threat source and the security controls currently implemented within the system as described in the security plan. The exploitation of an information system vulnerability (or vulnerabilities) by a threat source may be traced to one or more factors including: (i) the failure of currently implemented security controls; (ii) missing security controls; and/or (iii) insufficient strength of security controls. Using the results from the assessment of the current security state, the organization should reassess the risks posed to individuals, the organization, and its assets arising from use of the information system.

- Plan for and initiate any necessary corrective actions.

  Based on the results of an updated risk assessment, the organization should determine what additional security controls and/or control enhancements may be necessary to address the vulnerability (or vulnerabilities) related to the incident or what corrective actions may be needed to fix currently implemented controls deemed to be less than effective.

  The security plan for the information system should then be updated to reflect these corrective actions. A Plan of Action and Milestones (POA&M) should be developed for any deficiencies noted that are not immediately corrected and for the implementation of any security control upgrades or additional controls. After the security controls or control upgrades have been implemented and any other noted deficiencies corrected, the controls should be assessed for effectiveness. The assessment determines if the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the organization's security policy.

- Consider reaccrediting the information system.

  Depending on the severity of the incident, the impact on organizational operations, organizational assets, or individuals, and the extent of the corrective actions required to fix the identified deficiencies in the information system, the organization may need to consider reaccrediting the information system in accordance with the provisions of NIST Special

[41] Organizations should proactively initiate the actions in Section 3.5 when an organizational information system is believed to be at risk of targeted attacks based on law enforcement information, intelligence information, or other credible sources of information.

Publication 800-37. The authorizing official makes the final determination on the need to reaccredit the information system in consultation with the system and mission owners, the senior agency information security officer, and the chief information officer. The authorizing official may choose to conduct an abbreviated reaccreditation focusing only on the affected components of the information system and the associated security controls and/or control enhancements which have been changed during the update. Authorizing officials should have sufficient information from the security certification process to ensure with an appropriate degree of confidence, that in light of the incident, the necessary corrective actions have been taken and the organization's operations, assets, and individuals are adequately protected.

APPENDIX A

REFERENCES

LAWS, POLICIES, DIRECTIVES, MEMORANDA, STANDARDS, AND GUIDELINES

LEGISLATION

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
3. Paperwork Reduction Act of 1995 (P.L. 104-13), May 1995.
4. Privacy Act of 1974 (P.L. 93-579), ~~September~~ December 197~~5~~4.

POLICIES, DIRECTIVES, ~~POLICIES, AND INSTRUCTIONS~~ AND MEMORANDA

5. Department of Defense Instruction 8500.2, *Information Assurance Implementation*, February 2003.
6. Director of Central Intelligence Directive 6/3 Policy, *Protecting Sensitive Compartmented Information within Information Systems*, June 1999.
7. Director of Central Intelligence Directive 6/3 Manual, *Protecting Sensitive Compartmented Information within Information Systems*, May 2000.
8. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
9. Office of Management and Budget, Federal Enterprise Architecture Program Management Office, *Business Reference Model* (v2.0), June 2003.
10. Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.
11. Office of Management and Budget Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 2003.
12. Office of Management and Budget Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 2003.
13. Office of Management and Budget Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 2003.
14. Office of Management and Budget Memorandum M-0~~5~~6-~~15~~20, *FY 200~~5~~6 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, ~~June~~ July 200~~5~~6.
15. Office of Management and Budget Memorandum M-06-16, *Protection of Sensitive Information*, June 2006.
16. ~~Department of Defense Instruction 8500.2, *Information Assurance Implementation*, February 2003.~~
17. ~~Director of Central Intelligence Directive 6/3 Policy, *Protecting Sensitive Compartmented Information within Information Systems*, June 1999.~~

STANDARDS

18. International Organization for Standardization/International Electrotechnical Commission 27001, *Information Security Management System Requirements*, October 2005.

19. International Organization for Standardization/International Electrotechnical Commission 17799, *Code of Practice for Information Security Management*, June 2005.

20. National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001.

21. National Institute of Standards and Technology Federal Information Processing Standards Publication 180-2, *Secure Hash Standard (SHS)*, August 2002.

22. National Institute of Standards and Technology Federal Information Processing Standards Publication 186-2, *Digital Signature Standard (DSS)*, January 2000.

23. National Institute of Standards and Technology Federal Information Processing Standards Publication 188, *Standard Security Labels for Information Transfer*, September 1994.

24. National Institute of Standards and Technology Federal Information Processing Standards Publication 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, September 1994.

25. National Institute of Standards and Technology Federal Information Processing Standards Publication 197, *Advanced Encryption Standard (AES)*, November 2001.

26. National Institute of Standards and Technology Federal Information Processing Standards Publication 198, *The Keyed-Hash Message Authentication Code (HMAC)*, March 2002.

27. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

28. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, ~~February~~ March 2006.

29. National Institute of Standards and Technology Federal Information Processing Standards Publication 201-1, *Personal Identity Verification of Federal Employees and Contractors*, ~~February~~ March 200~~5~~6.

30. Committee for National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, ~~May~~ June 200~~3~~6.

31. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, *Protective Distribution Systems (PDS)*, December 1996.

GUIDELINES

32. National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

33. National Institute of Standards and Technology Special Publication 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network*, October 1995.

34. National Institute of Standards and Technology Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.

35. National Institute of Standards and Technology Special Publication 800-15, *Minimum Interoperability Specification for PKI Components (MISPC)*, Version 1, September 1997.

36. National Institute of Standards and Technology Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998.

37. National Institute of Standards and Technology Special Publication 800-17, *Modes of Operation Validation System (MOVS): Requirements and Procedures*, February 1998.

38. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

39. National Institute of Standards and Technology Special Publication 800-19, *Mobile Agent Security*, October 1999.

40. National Institute of Standards and Technology Special Publication 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures*, April 2000.

41. National Institute of Standards and Technology Special Publication 800-21-1, *Second Edition, Guideline for Implementing Cryptography in the Federal Government*, December 2005.

42. National Institute of Standards and Technology Special Publication 800-22, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, May 2001.

43. National Institute of Standards and Technology Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.

~~44. National Institute of Standards and Technology Special Publication 800-26, Revision 1 (Draft), *Guide for Information Security Program Assessments and System Reporting Form*, August 2005.~~

45. National Institute of Standards and Technology Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, Revision A, June 2004.

46. National Institute of Standards and Technology Special Publication 800-28, *Guidelines on Active Content and Mobile Code*, October 2001.

47. National Institute of Standards and Technology Special Publication 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001.

48. National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

49. National Institute of Standards and Technology Special Publication 800-31, *Intrusion Detection Systems (IDS)*, November 2001.

50. National Institute of Standards and Technology Special Publication 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001.

51. National Institute of Standards and Technology Special Publication 800-33, *Underlying Technical Models for Information Technology Security*, December 2001.

52. National Institute of Standards and Technology Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

53. National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003.

54. National Institute of Standards and Technology Special Publication 800-36, *Guide to Selecting Information Security Products*, October 2003.

55. National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

56. National Institute of Standards and Technology Special Publication 800-38A, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*, December 2001.

57. National Institute of Standards and Technology Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005.

58. National Institute of Standards and Technology Special Publication 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*, May 2004.

59. National Institute of Standards and Technology Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication* (Draft), April 2006.

60. National Institute of Standards and Technology Special Publication 800-40, Version 2.0, *Creating a Patch and Vulnerability Management Program*, November 2005.

61. National Institute of Standards and Technology Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002.

62. National Institute of Standards and Technology Special Publication 800-42, *Guideline on Network Security Testing*, October 2003.

63. National Institute of Standards and Technology Special Publication 800-43, *Systems Administration Guidance for Windows 2000 Professional*, November 2002.

64. National Institute of Standards and Technology Special Publication 800-44, *Guidelines on Securing Public Web Servers*, September 2002.

65. National Institute of Standards and Technology Special Publication 800-45, *Guidelines on Electronic Mail Security*, September 2002.

66. National Institute of Standards and Technology Special Publication 800-46, *Security for Telecommuting and Broadband Communications*, August 2002.

67. National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

68. National Institute of Standards and Technology Special Publication 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*, November 2002.

69. National Institute of Standards and Technology Special Publication 800-49, *Federal S/MIME V3 Client Profile*, November 2002.

70. National Institute of Standards and Technology Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.

71. National Institute of Standards and Technology Special Publication 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, September 2002.

72. National Institute of Standards and Technology Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, June 2005.

73. National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (~~s~~Second ~~p~~Public ~~d~~Draft), ~~spring~~ April 2006~~)~~.

74. National Institute of Standards and Technology Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003.

75. National Institute of Standards and Technology Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, ~~(final public draft) July 2005~~ March 2006.

76. National Institute of Standards and Technology Special Publication 800-57, *Recommendation on Key Management*, August 2005.

77. National Institute of Standards and Technology Special Publication 800-58, *Security Considerations for Voice Over IP Systems*, January 2005.

78. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

79. National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

80. National Institute of Standards and Technology Special Publication 800-61, *Computer Security Incident Handling Guide*, January 2004.

81. National Institute of Standards and Technology Special Publication 800-63, Version 1.0.~~1~~2, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Guidelines*, ~~September~~ April 200~~4~~6.

82. National Institute of Standards and Technology Special Publication 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004.

83. National Institute of Standards and Technology Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005.

84. National Institute of Standards and Technology Special Publication 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005.

85. National Institute of Standards and Technology Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, May 2004.

86. National Institute of Standards and Technology Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2005.

87. National Institute of Standards and Technology Special Publication 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*, May 2005.

88. National Institute of Standards and Technology Special Publication 800-72, *Guidelines on PDA Forensics*, November 2004.

89. National Institute of Standards and Technology Special Publication 800-73, Revision 1, *Interfaces for Personal Identity Verification*, April 200~~5~~6.

90. National Institute of Standards and Technology Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*, February 2006.

91. National Institute of Standards and Technology Special Publication 800-77, *Guide to IPsec VPNs*, December 2005.

92. National Institute of Standards and Technology Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, April 2005.

93. National Institute of Standards and Technology Special Publication 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, July 2005.

94. National Institute of Standards and Technology Special Publication 800-80, *Guide for Developing Performance Metrics for Information Security* (Draft), May 2006.

95. National Institute of Standards and Technology Special Publication 800-81, *Secure Domain Name System (DNS) Deployment Guide* ~~(Draft), August 2005~~, May 2006.

96. National Institute of Standards and Technology Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005.

97. National Institute of Standards and Technology Special Publication 800-85A, ~~*PIV Middleware and*~~ *PIV Card Application* ~~*Conformance*~~ *and Middleware Interface Test Guidelines*, ~~October~~ April 200~~5~~6.

98. National Institute of Standards and Technology Special Publication 800-85B, *PIV Data Model Test Guidelines* (Draft), May 2006.

99. National Institute of Standards and Technology Special Publication 800-86, *Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response* (Draft), August 2005.

100. National Institute of Standards and Technology Special Publication 800-87, *Codes for the Identification of Federal and Federally-Assisted Organizations*, January 2006.

101. National Institute of Standards and Technology Special Publication 800-88, *Guidelines for Media Sanitization* (Draft), February 2006.

102. National Institute of Standards and Technology Special Publication 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications* (Draft), March 2006.

103. National Institute of Standards and Technology Special Publication 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, June 2006.

104. National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Security Log Management* (Draft), April 2006.

105. National Institute of Standards and Technology Special Publication 800-96, *PIV Card / Reader Interoperability Guidelines* (Draft), May 2006.

106. National Institute of Standards and Technology Special Publication 800-97, *Guide to IEEE 802.11i: Establishing Robust Security Networks* (Draft), June 2006.

107. National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers* (Draft), June 2006.

MISCELLANEOUS PUBLICATIONS

108. Department of Health and Human Services Centers for Medicare and Medicaid Services (CMS), *Core Set of Security Requirements*, February 2004.

~~109. Director of Central Intelligence Directive 6/3 Manual, *Protecting Sensitive Compartmented Information within Information Systems*, May 2000.~~

110. Government Accountability Office, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6, January 1999.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix B provides definitions for security terminology used within Special Publication 800-53. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in CNSS Instruction 4009, *National Information Assurance Glossary*.

Accreditation
[NIST SP 800-37]

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

Accreditation Boundary
[NIST SP 800-37]

All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3.

Accrediting Authority

See Authorizing Official.

Adequate Security
[OMB Circular A-130, Appendix III]

Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Agency

See Executive Agency.

Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authenticity

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.

Authorize Processing

See Accreditation.

Authorizing Official
[NIST SP 800-37]

Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

Availability
[44 U.S.C., Sec. 3542]

Ensuring timely and reliable access to and use of information.

Boundary Protection

Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels).

Certification
[NIST SP 800-37]

A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Certification Agent
[NIST SP 800-37]

The individual, group, or organization responsible for conducting a security certification.

Certification Practice Statement

A statement of the practices that a Certification Authority employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in a certificate policy~~,~~ or requirements specified in a contract for services).

Chief Information Officer
[~~44 U.S.C.~~ PL 104-106, Sec. 5125(b)]

Agency official responsible for:

(i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency;

(ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and

(iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

Common Security Control
[NIST SP 800-37]

Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.

Compensating Security Controls

The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.

Confidentiality
[44 U.S.C., Sec. 3542]

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Control
[CNSS Inst. 4009]

Process for controlling modifications to hardware, firmware, software, and documentation to ensure that the information system is protected against improper modifications before, during, and after system implementation.

Countermeasures
[CNSS Inst. 4009]

Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.

Controlled Interface
[CNSS Inst. 4009]

Mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system).

Executive Agency
[41 U.S.C., Sec. 403]

An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

Federal Enterprise Architecture
[FEA Program Management Office]

A business-based framework for governmentwide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.

Federal Information System
[40 U.S.C., Sec. 11331]

An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

General Support System
[OMB Circular A-130, Appendix III]

An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

Guard (System)
[CNSS Inst. 4009, Adapted]

A mechanism limiting the exchange of information between information systems or subsystems.

High-Impact System

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.

Industrial Control System

An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes.

Information Owner
[CNSS Inst. 4009]

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Resources
[44 U.S.C., Sec. 3502]

Information and related resources, such as personnel, equipment, funds, and information technology.

Information Security
[44 U.S.C., Sec. 3542]

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Policy
[CNSS Inst. 4009]

Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Information System
[44 U.S.C., Sec. 3502]
[OMB Circular A-130, Appendix III]

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Owner (or Program Manager)
[CNSS Inst. 4009, Adapted]

Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information System Security Officer
[CNSS Inst. 4009, Adapted]

Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program.

Information Technology
[40 U.S.C., Sec. 1401]

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Information Type
[FIPS 199]

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Integrity
[44 U.S.C., Sec. 3542]

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Label

See Security Label.

Low-Impact System

An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.

Major Application
[OMB Circular A-130, Appendix III]

An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

Major Information System
[OMB Circular A-130]

An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

Malicious Code
[CNSS Inst. 4009]
[NIST SP 800-61]

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Malware

See Malicious Code.

Management Controls
[NIST SP 800-18, Rev 1]

The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

Media Access Control Address

A hardware address that uniquely identifies each component of an IEEE 802-based network. On networks that do not conform to the IEEE 802 standards but do conform to the OSI Reference Model, the node address is called the Data Link Control (DLC) address.

Media Sanitization
~~[CNSS Inst. 4009, Adapted]~~
[NIST SP 800-88]

~~Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.~~ A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

Mobile Code

Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.

Mobile Code Technologies

Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).

Moderate-Impact System

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.

National Security Emergency Preparedness Telecommunications Services
[47 C.F.R., Part 64, App A]

Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.

National Security Information

Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

National Security System
[44 U.S.C., Sec. 3542]

Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Non-repudiation
[CNSS Inst. 4009]

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

Operational Controls
[NIST SP 800-18, Rev 1]

The security controls (i.e., safeguards or countermeasures) for an information system that are primarily ~~are~~ implemented and executed by people (as opposed to systems).

Plan of Action and Milestones
[OMB Memorandum 02-01]

A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Potential Impact
[FIPS 199]

The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS 199 low); (ii) a *serious* adverse effect (FIPS 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.

Privacy Impact Assessment
[OMB Memorandum 03-22]

An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Protective Distribution System

Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.

Records

The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

Remote Access

Access by users (or information systems) communicating external to an information system security perimeter.

Remote Maintenance

Maintenance activities conducted by individuals communicating external to an information system security perimeter.

Risk
[NIST SP 800-30]

The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Risk Assessment
[NIST SP 800-30, Adapted]

The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals ~~by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact~~ arising through the operation of the information system. Part of risk management, synonymous with risk analysis, ~~and~~ incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in place security controls.

Risk Management
[NIST SP 800-30, Adapted]

The process of ~~managing~~ assessing and mitigating risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. The process includes: security categorization of the information system; the selection and tailoring of minimum (baseline) security controls; the assessment of organizational risk to determine the sufficiency of controls; the documentation of security controls in the system security plan; the implementation of security controls and the assessment of control effectiveness; the authorization to operate the information system based on an acceptance of residual risk; and the continuous monitoring of security controls. ~~It includes: risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.~~

Safeguards
[CNSS Inst. 4009, Adapted]

Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Scoping Guidance

Provides organizations with specific policy/regulatory-related, technology-related, physical infrastructure-related, operational/environmental-related, public access-related, scalability-related, common security control-related, and ~~risk~~security objective-related considerations on the applicability and implementation of individual security controls in the control baseline.

Security Category
[FIPS 199]

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

Security Controls
[FIPS 199]

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Control Baseline

The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

Security Control Enhancements

Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.

Security Functions

The hardware, software, and firmware of the information system responsible for supporting and enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

Security Impact Analysis
[NIST SP 800-37]

The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.

Security Label

Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein.

Security Objective

Confidentiality, integrity, or availability.

Security Perimeter

See Accreditation Boundary.

Security Plan

See System Security Plan.

Security Requirements

Requirements levied on an information system that are derived from laws, Executive Orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure that the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Senior Agency Information Security Officer
[44 U.S.C., Sec. 3544]

Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.

Spyware

Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

Subsystem

A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.

System

See Information System.

System-specific Security Control
[NIST SP 800-37]

A security control for an information system that has not been designated as a common security control.

System Security Plan
[NIST SP 800-18, Rev 1]

Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Tailoring

The process by which a security control baseline selected in accordance with the FIPS 199 security categorization of the information system is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls, where allowed.

Tailored Security Control Baseline

Set of security controls resulting from the application of the tailoring guidance to the security control baseline.

Technical Controls
[NIST SP 800-18, Rev 1]

The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Threat
[CNSS Inst. 4009, Adapted]

Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat Agent/Source
[NIST SP 800-30]

Either: (i) intent and method targeted at the intentional exploitation of a vulnerability; or (ii) a situation and method that may accidentally trigger a vulnerability.

Threat Assessment
[CNSS Inst. 4009]

Formal description and evaluation of threat to an information system.

Trusted Path

A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software.

User
[CNSS Inst. 4009]

Individual or (system) process authorized to access an information system.

Vulnerability
[CNSS Inst. 4009, Adapted]

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Assessment
[CNSS Inst. 4009]

Formal description and evaluation of the vulnerabilities in an information system.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CFR	Code of Federal Regulations
CIO	Chief Information Officer
CNSS	Committee for National Security Systems
~~COTS~~	~~Commercial Off-The-Shelf~~
DCID	Director of Central Intelligence Directive
DNS	Domain Name System
~~FEA~~	~~Federal Enterprise Architecture~~
FIPS	Federal Information Processing Standard(s)
FISMA	Federal Information Security Management Act
~~GOTS~~	~~Government Off-The-Shelf~~
IEEE	Institute of Electrical and Electronics Engineers
IPsec	Internet Protocol Security
~~IPv6~~	~~Internet Protocol Version 6~~
~~MAC~~	~~Media Access Control~~
~~MOA~~	~~Memorandum of Agreement~~
~~MOU~~	~~Memorandum of Understanding~~
NIST	National Institute of Standards and Technology
~~NSA~~	~~National Security Agency~~
NSTISSI	National Security Telecommunications and Information System Security Instruction
OMB	Office of Management and Budget
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
POAM	Plan of Action and Milestones
SP	Special Publication
~~TCP/IP~~	~~Transmission Control Protocol/Internet Protocol~~
~~TLS~~	~~Transport Layer Security~~
TSP	Telecommunications Service Priority
~~USC~~	~~United States Code~~
VPN	Virtual Private Network

VoIP	Voice over Internet Protocol

APPENDIX D

MINIMUM SECURITY CONTROLS – SUMMARY

LOW-IMPACT, MODERATE-IMPACT, AND HIGH-IMPACT INFORMATION SYSTEMS

The following table lists the minimum security controls, or security control baselines, for low-impact, moderate-impact, and high-impact information systems. If a security control is selected for one of the baselines, the family identifier and control number are listed in the appropriate column. If a control is not used in a particular baseline, the entry is marked "not selected." Control enhancements, when used to supplement basic security controls, are indicated by the number of the control enhancement. For example, an "IR-2 (1)" in the high baseline entry for the IR-2 security control indicates that the second control from the Incident Response family has been selected along with control enhancement (1). Some security controls and control enhancements in the security control catalog are not used in any of the baselines but are available for ~~optional~~ use by organizations ~~when indicated~~ if needed; for example, ~~based on~~ when the results of a risk assessment indicate the need for additional controls or control enhancements in order to adequately mitigate risks to individuals, the organization, or its assets. A complete description of security controls, supplemental guidance for the controls, and control enhancements is provided in Appendix F. A detailed listing of security controls and control enhancements for each control baseline is available at: http://csrc.nist.gov/sec-cert.

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
Access Control				
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6	AC-6
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-9	Previous Logon Notification	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	Not Selected	Not Selected	AC-10
AC-11	Session Lock	Not Selected	AC-11	AC-11
AC-12	Session Termination	Not Selected	AC-12	AC-12 (1)
AC-13	Supervision and Review—Access Control	AC-13	AC-13 (1)	AC-13 (1)
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking	Not Selected	Not Selected	AC-15
AC-16	Automated Labeling	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access Restrictions	AC-18	AC-18 (1)	AC-18 (1) (2)
AC-19	Access Control for Portable and Mobile Systems	Not Selected	AC-19 (1)	AC-19 (1)
AC-20	~~Personally Owned~~ Use of External Information Systems	AC-20	AC-20 (1)	AC-20 (1) (2)
Awareness and Training				
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1
AT-2	Security Awareness	AT-2	AT-2	AT-2
AT-3	Security Training	AT-3	AT-3	AT-3
AT-4	Security Training Records	AT-4	AT-4	AT-4
AT-5	Contacts with Security Groups and Associations	Not Selected	Not Selected	Not Selected
Audit and Accountability				
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1
AU-2	Auditable Events	AU-2	AU-2 (3)	AU-2 (1) (2) (3)
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Monitoring, Analysis, and Reporting	Not Selected	AU-6 (2)	AU-6 (1) (2)
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7 (1)	AU-7 (1)

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	**MOD**	**HIGH**
AU-8	Time Stamps	~~Not Selected~~ AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9	AU-9
AU-10	Non-repudiation	Not Selected	Not Selected	Not Selected
AU-11	Audit Record Retention	AU-11	AU-11	AU-11
	Certification, Accreditation, and Security Assessments			
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	CA-1	CA-1	CA-1
CA-2	Security Assessments	Not Selected	CA-2	CA-2
CA-3	Information System Connections	CA-3	CA-3	CA-3
CA-4	Security Certification	CA-4	CA-4 (1)	CA-4 (1)
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5
CA-6	Security Accreditation	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7	CA-7
	Configuration Management			
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1
CM-2	Baseline Configuration and System Component Inventory	CM-2	CM-2 (1)	CM-2 (1) (2)
CM-3	Configuration Change Control	Not Selected	CM-3	CM-3 (1)
CM-4	Monitoring Configuration Changes	Not Selected	CM-4	CM-4
CM-5	Access Restrictions for Change	Not Selected	CM-5	CM-5 (1)
CM-6	Configuration Settings	CM-6	CM-6	CM-6 (1)
CM-7	Least Functionality	Not Selected	CM-7	CM-7 (1)
	Contingency Planning			
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1)	CP-2 (1) (2) (3)
CP-3	Contingency Training	Not Selected	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	Not Selected	CP-4 (1)	CP-4 (1) (2)
CP-5	Contingency Plan Update	CP-5	CP-5	CP-5
CP-6	Alternate Storage Sites	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Sites	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1) (4)	CP-9 (1) (2) (3) (4)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10	CP-10 (1)
	Identification and Authentication			
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1
IA-2	User Identification and Authentication	IA-2	IA-2	IA-2 (1)

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4	IA-4
IA-5	Authenticator Management	IA-5	IA-5	IA-5
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7
Incident Response				
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1
IR-2	Incident Response Training	Not Selected	IR-2	IR-2 (1)
IR-3	Incident Response Testing	Not Selected	IR-3	IR-3 (1)
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	Not Selected	IR-5	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (1)	IR-7 (1)
Maintenance				
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1
MA-2	Periodic Maintenance	MA-2	MA-2 (1)	MA-2 (1) (2)
MA-3	Maintenance Tools	Not Selected	MA-3	MA-3 (1) (2) (3)
MA-4	Remote Maintenance	MA-4	MA-4	MA-4 (1) (2) (3)
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5 (1)
MA-6	Timely Maintenance	Not Selected	MA-6	MA-6
Media Protection				
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2 (1)	MP-2 (1)
MP-3	Media Labeling	Not Selected	MP-3	MP-3
MP-4	Media Storage	Not Selected	MP-4 (1)	MP-4 (1)
MP-5	Media Transport	Not Selected	MP-5 (1)	MP-5 (1) (2)
MP-6	Media Sanitization and Disposal	MP-6	MP-6	MP-6 (1) (2)
Physical and Environmental Protection				
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	Not Selected	Not Selected	PE-4
PE-5	Access Control for Display Medium	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6 (1)	PE-6 (1) (2)
PE-7	Visitor Control	PE-7	PE-7 (1)	PE-7 (1)
PE-8	Access ~~Logs~~ Records	PE-8	PE-8	PE-8 (1) (2)
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	Not Selected	PE-10	PE-10 (1)

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-11	Emergency Power	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12
PE-13	Fire Protection	PE-13	PE-13 (1) (2) (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	PE-18	PE-18 (1)
PE-19	Information Leakage	Not Selected	Not Selected	Not Selected
Planning				
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2	PL-2
PL-3	System Security Plan Update	PL-3	PL-3	PL-3
PL-4	Rules of Behavior	PL-4	PL-4	PL-4
PL-5	Privacy Impact Assessment	PL-5	PL-5	PL-5
PL-6	Security-Related Activity Planning	Not Selected	PL-6	PL-6
Personnel Security				
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1
PS-2	Position Categorization	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3	PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4
PS-5	Personnel Transfer	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8
Risk Assessment				
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3
RA-4	Risk Assessment Update	RA-4	RA-4	RA-4
RA-5	Vulnerability Scanning	Not Selected	RA-5	RA-5 (1) (2)
System and Services Acquisition				
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	Life Cycle Support	SA-3	SA-3	SA-3
SA-4	Acquisitions	SA-4	SA-4	SA-4
SA-5	Information System Documentation	SA-5	SA-5 (1)	SA-5 (1) (2)
SA-6	Software Usage Restrictions	SA-6	SA-6	SA-6

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-7	User Installed Software	SA-7	SA-7	SA-7
SA-8	Security ~~Design~~ Engineering Principles	Not Selected	SA-8	SA-8
SA-9	Outsourced Information System Services	SA-9	SA-9	SA-9
SA-10	Developer Configuration Management	Not Selected	Not Selected	SA-10
SA-11	Developer Security Testing	Not Selected	SA-11	SA-11
System and Communications Protection				
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected	Not Selected	SC-3
SC-4	Information Remnants	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5
SC-6	Resource Priority	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	SC-7	SC-7 (1) (2) (3)	SC-7 (1) (2) (3) (4)
SC-8	Transmission Integrity	Not Selected	SC-8	SC-8 (1)
SC-9	Transmission Confidentiality	Not Selected	SC-9	SC-9 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10
SC-11	Trusted Path	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Mgmt.	Not Selected	SC-12	SC-12
SC-13	Use of Validated Cryptography	SC-13	SC-13	SC-13
SC-14	Public Access Protections	SC-14	SC-14	SC-14
SC-15	Collaborative Computing	Not Selected	SC-15	SC-15
SC-16	Transmission of Security Parameters	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17
SC-18	Mobile Code	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	SC-19	SC-19
SC-20	Secure Name ~~Lookup~~ /Address Resolution Service (Authoritative Source)	Not Selected	SC-20	SC-20
SC-21	Secure Name ~~Lookup~~ /Address Resolution Service (~~Resolution~~ Recursive or Caching Resolver)	Not Selected	Not Selected	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	Not Selected	SC-22	SC-22
SC-23	Session Authenticity	Not Selected	SC-23	SC-23 (1)
System and Information Integrity				
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	SI-3	SI-3 (1)	SI-3 (1) (2)
SI-4	Information System Monitoring Tools and Techniques	Not Selected	SI-4 (4)	SI-4 (2) (4) (5)

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-5	Security Alerts and Advisories	SI-5	SI-5	SI-5 (1)
SI-6	Security Functionality Verification	Not Selected	Not Selected	SI-6
SI-7	Software and Information Integrity	Not Selected	Not Selected	SI-7
SI-8	Spam Protection	Not Selected	SI-8	SI-8 (1)
SI-9	Information Input Restrictions	Not Selected	SI-9	SI-9
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	Not Selected	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11
SI-12	Information Output Handling and Retention	Not Selected	SI-12	SI-12

APPENDIX E

MINIMUM ASSURANCE REQUIREMENTS

LOW, MODERATE, AND HIGH BASELINE APPLICATIONS

The minimum assurance requirements for security controls described in the security control catalog are listed below. The assurance requirements are directed at the activities and actions that security control developers and implementers[42] define and apply to increase the level of confidence that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. The assurance requirements are applied on a control-by-control basis. The requirements are grouped by security control baseline (i.e., low, moderate, and high) since the requirements apply to each control within the respective baseline. Using a format similar to security controls, assurance requirements are followed by supplemental guidance that provides additional detail and explanation of how the requirements are to be applied. Bolded text indicates requirements that appear for the first time in a particular baseline.

Low Baseline

Assurance Requirement: **The security control is in effect and meets explicitly identified functional requirements in the control statement.**

Supplemental Guidance: For security controls in the low baseline, the focus is on the control being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner.

Moderate Baseline

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. **The control developer/implementer provides a description of the functional properties of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions to ensure that when the control is implemented, it will meet its required function or purpose. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.**

Supplemental Guidance: For security controls in the moderate baseline, the focus is on ensuring correct implementation and operation of the control. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer/implementer incorporates, as part of the control, specific capabilities and produces specific documentation to ensure that the control meets its required function or purpose. This documentation is also needed by assessors to analyze and test the functional properties of the control as part of the overall assessment of the control.

High Baseline

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties **and design/implementation** of the control with sufficient detail to permit analysis and testing of the control (**including functional interfaces among control components)**. The control

[42] In this context, a developer/implementer is an individual or group of individuals responsible for the development or implementation of security controls for an information system. This may include, for example, hardware and software vendors providing the controls, contractors implementing the controls, or organizational personnel such as information system owners, information system security officers, system and network administrators, or other individuals with security responsibility for the information system.

developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions to ensure that when the control is implemented, it will **continuously and consistently (i.e., across the information system)** meet its required function or purpose **and support improvement in the effectiveness of the control**. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

Supplemental Guidance: For security controls in the high baseline, the focus is expanded to require, within the control, the capabilities that are needed to support ongoing consistent operation of the control and continuous improvement in the control's effectiveness. The developer/implementer is expected to expend significant effort on the design, development, implementation, and component/integration testing of the controls and to produce associated design and implementation documentation to support these activities. ~~For security controls in the high baseline, t~~This ~~same~~ documentation is also needed by assessors to analyze and test the internal components of the control as part of the overall assessment of the control.

Additional Requirements Enhancing the Moderate and High Baselines

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, actions to ensure that when the control is implemented, it will continuously and consistently (i.e., across the information system) meet its required function or purpose and support improvement in the effectiveness of the control. These actions include requiring the development of records with structure and content suitable to facilitate making this determination. **The control is developed in a manner that supports a high degree of confidence that the control is complete, consistent, and correct.**

Supplemental Guidance: The additional high assurance requirements are intended to supplement the minimum assurance requirements for the moderate and high baselines, when appropriate, in order to protect against threats from highly skilled, highly motivated, and well-financed threat agents. This level of protection is ~~required~~ necessary for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above.

APPENDIX F

SECURITY CONTROL CATALOG

SECURITY CONTROLS, SUPPLEMENTAL GUIDANCE, AND CONTROL ENHANCEMENTS

The following catalog of security controls provides a range of safeguards and countermeasures for information systems. The security controls are organized into *families* for ease of use in the control selection and specification process. Each family contains security controls related to the security functionality of the family. A standardized, two-character identifier is assigned to uniquely identify each control family. To uniquely identify each control, a numeric identifier is appended to the family identifier to indicate the number of the control within the control family.

The security control structure consists of three key components: (i) a *control* section; (ii) a *supplemental guidance* section; and (iii) a *control enhancements* section. The control section provides a concise statement of the specific security capability needed to protect a particular aspect of an information system. The control statement describes specific security-related activities or actions to be carried out by the organization or by the information system. For some controls in the control catalog, a degree of flexibility is provided by allowing organizations to selectively define input values for certain parameters associated with the controls. This flexibility is achieved through the use of *assignment* and *selection* operations within the control.

The supplemental guidance section provides additional information related to a specific security control. Organizations should consider supplemental guidance when defining, developing, and implementing security controls. Applicable federal legislation, Executive Orders, directives, policies, regulations, standards, and guidance documents (e.g., OMB Circulars, FIPS, and NIST Special Publications) are listed in the supplemental guidance section, when appropriate, for the particular security control.[43] In certain instances, the supplemental guidance provides important considerations (and the needed flexibility) for implementing security controls in the context of an organization's operational environment, specific mission requirements, or assessment of risk.

The control enhancements section provides statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control. In both cases, the control enhancements are used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additions to a basic control's functionality based on the results of a risk assessment. Control enhancements are numbered sequentially within each control so the enhancements can be easily identified when selected to supplement the basic control. The numerical designation of a security control enhancement is used only to identify a particular enhancement within the control structure. The designation is neither indicative of the relative strength of the control enhancement nor assumes any hierarchical relationship among enhancements. The three security control baselines described in Chapter Three are hierarchical in nature and therefore, the security controls and control enhancements in those baselines are supersets of each other, moving from the low to the moderate to the high baseline.

[43] NIST Special Publications listed in the supplemental guidance sections of security controls are assumed to refer to the most recent updates to those publications. For example, a reference to NIST Special Publication 800-18 refers to the Special Publication 800-18, Revision 1, which is the latest version of the security planning guideline.

Cautionary Note

The security controls described in this catalog should be employed in federal information systems in accordance with the risk management guidance provided in Chapter ~~3~~ Three. This guidance includes the selection of minimum (baseline) security controls based upon the FIPS 199 security categorization of the information system and the tailoring of the minimum (baseline) security controls by: (i) applying appropriate scoping guidance; (ii) specifying compensating controls, if needed; ~~(iii) specifying additional security controls when required;~~ and (i~~v~~ii) inserting organization-defined security control parameters, where allowed. ~~***Not all security controls defined in the catalog are used in the minimum security control baselines.***~~ ~~Additional security controls are available and can be selected and employed by organizations as needed in accordance with an organizational assessment of risk.~~ Since the baseline security controls represent the minimum controls for low-impact, moderate-impact, and high-impact information systems, respectively, there are additional controls and control enhancements that appear in the catalog that are not used in any of the baselines. These additional security controls and control enhancements are available to organizations and can be used in supplementing the tailored baselines to achieve the needed level of protection in accordance with an organizational assessment of risk. Moreover, security controls and control enhancements contained in higher-level baselines can also be used by organizations to strengthen the level of protection provided in lower-level baselines, if deemed appropriate.

With regard to cryptography employed in federal information systems, organizations must comply with current federal policy and meet the requirements of FIPS 140-2 (as amended), *Security Requirements for Cryptographic Modules*. Cryptographic module validation certificates issued by the Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2 and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. The FIPS 140-2 standard also acknowledges the use of cryptography approved by the National Security Agency as an appropriate alternative for organizations. Consult FIPS 140-2 for specific guidance.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Supplemental Guidance: The access control policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW AC-1	**MOD** AC-1	**HIGH** AC-1

AC-2 ACCOUNT MANAGEMENT

Control: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [*Assignment: organization-defined frequency*, *at least annually*].

Supplemental Guidance: Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. The organization ensures that account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know changes.

Control Enhancements:

(1) **The organization employs automated mechanisms to support the management of information system accounts.**

(2) **The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].**

(3) **The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*].**

(4) **The organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified.**

LOW AC-2	**MOD** AC-2 (1) (2) (3) (4)	**HIGH** AC-2 (1) (2) (3) (4)

AC-3 ACCESS ENFORCEMENT

Control: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, ruled-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant. If the federal Personal Identity Verification (PIV) credential is used as an identification token where token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publication 800-73 and employs either cryptographic verification or biometric verification. If the token-based access control employs cryptographic verification, the access control system conforms to the requirements of NIST Special Publication 800-78. If the token-based access control employs biometric verification, the access control system conforms to the requirements of NIST Special Publication 800-76.

Control Enhancements:

(1) The information system ensures that access to security functions (deployed in hardware, software, and firmware) and security-relevant information is restricted to explicitly authorized personnel (e.g., security administrators, system and network administrators, and other privileged users).

LOW AC-3	**MOD** AC-3 (1)	**HIGH** AC-3 (1)

AC-4 INFORMATION FLOW ENFORCEMENT

Control: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Supplemental Guidance: Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems ~~based on the characteristics of the information~~. This control is based on the characteristics of the information and/or the information path. ~~Simple~~ Common examples of flow control enforcement can be found in firewall and router devices that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability. ~~Flow control enforcement can also be found in information systems that use explicit labels on information, source, and destination objects as the basis for flow control decisions (e.g., to control the release of certain types of information).~~

Control Enhancements: ~~None.~~

(1) Label-based control: Flow control enforcement uses explicit labels on information, source, and destination objects as a basis for flow control decisions (e.g., to control the release of certain types of information).

(2) Domain-based control: Flow control enforcement uses protected processing domains (e.g., type-enforcement) as a basis for flow control decisions.

LOW Not Selected	**MOD** AC-4	**HIGH** AC-4

AC-5 SEPARATION OF DUTIES

Control: The information system enforces separation of duties through assigned access authorizations.

Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.

Control Enhancements: None.

LOW Not Selected	**MOD** AC-5	**HIGH** AC-5

AC-6 LEAST PRIVILEGE

Control: The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Supplemental Guidance: The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

Control Enhancements: None.

LOW Not Selected	**MOD** AC-6	**HIGH** AC-6

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Control: The information system enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*] time period. The information system automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*], *delays next login prompt according to* [*Assignment: organization-defined delay algorithm.*]] when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.

Control Enhancements:

(1) The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

LOW AC-7	**MOD** AC-7	**HIGH** AC-7

AC-8 SYSTEM USE NOTIFICATION

Control: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Supplemental Guidance: Privacy and security policies are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available as opposed to displaying the information before granting access; (ii) there are no references to monitoring, recording, or auditing since privacy accommodations for such systems generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

Control Enhancements: None.

LOW AC-8	**MOD** AC-8	**HIGH** AC-8

AC-9 PREVIOUS LOGON NOTIFICATION

Control: The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-10 CONCURRENT SESSION CONTROL

Control: The information system limits the number of concurrent sessions for any user to [*Assignment: organization-defined number of sessions*].

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** AC-10

AC-11 SESSION LOCK

Control: The information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

Supplemental Guidance: Users can directly initiate session lock mechanisms. The information system also activates session lock mechanisms automatically after a specified period of inactivity defined by the organization. A session lock is not a substitute for logging out of the information system.

Control Enhancements: None.

LOW Not Selected	**MOD** AC-11	**HIGH** AC-11

AC-12 SESSION TERMINATION

Control: The information system automatically terminates a session after [*Assignment: organization-defined time period*] of inactivity.

Supplemental Guidance: ~~None~~ The session termination control only applies to remote sessions unless the control enhancement is selected.

Control Enhancements: ~~None.~~

(1) Automatic session termination applies to local and remote sessions.

LOW Not Selected	**MOD** AC-12	**HIGH** AC-12 (1)

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

Control: The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.

Supplemental Guidance: The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities. The extent of the audit record reviews is based on the FIPS 199 impact level of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records. NIST Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the review of user activities.

LOW AC-13	**MOD** AC-13 (1)	**HIGH** AC-13 (1)

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control: The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.

Supplemental Guidance: The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems.

Control Enhancements:

(1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

LOW AC-14	**MOD** AC-14 (1)	**HIGH** AC-14 (1)

AC-15 AUTOMATED MARKING

Control: The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

Supplemental Guidance: Automated marking refers to ~~labels~~ markings employed on external media (e.g., hardcopy documents output from the information system). The ~~labels~~ markings used in external marking are distinguished from the labels used on internal data structures described in AC-16.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** AC-15

AC-16 AUTOMATED LABELING

Control: The information system appropriately labels information in storage, in process, and in transmission.

Supplemental Guidance: Automated labeling refers to labels employed on internal data structures (e.g., records, files) within the information system. Information labeling is accomplished in accordance with: (i) access control requirements; (ii) special dissemination, handling, or distribution instructions; or (iii) as otherwise required to enforce information system security policy.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-17 REMOTE ACCESS

Control: The organization documents, monitors, and controls all methods of remote access (e.g., dial-up, broadband, Internet) to the information system ~~including remote access for privileged functions~~. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.

Supplemental Guidance: Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). ~~The organization permits remote access for privileged functions only for compelling operational needs.~~ NIST Special Publication 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publications 800-73 and 800-78. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

(2) The organization uses encryption to protect the confidentiality of remote access sessions.

(3) The organization controls all remote accesses through a limited number of managed access control points.

(4) The organization permits remote access for privileged functions only for compelling operational needs.

LOW AC-17	**MOD** AC-17 (1) (2) (3) (4)	**HIGH** AC-17 (1) (2) (3) (4)

AC-18 WIRELESS ACCESS RESTRICTIONS

Control: The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) documents, monitors, and controls wireless access to the information system. Appropriate organizational officials authorize the use of wireless technologies.

Supplemental Guidance: NIST Special Publications 800-48 and 800-97 provide~~s~~ guidance on wireless network security.

Control Enhancements:

(1) The organization uses authentication and encryption to protect wireless access to the information system.

(2) The organization scans for unauthorized wireless access points [*Assignment: organization-defined frequency*] and takes appropriate action if such an access points are discovered.

Enhancement Supplemental Guidance: Organizations conduct a thorough scan for unauthorized wireless access points in facilities containing high-impact information systems. The scan is not limited to only those areas within the facility containing the high-impact information systems.

LOW AC-18	**MOD** AC-18 (1)	**HIGH** AC-18 (1) (2)

AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES

Control: The organization: (i) establishes usage restrictions and implementation guidance for portable and mobile devices; and (ii) documents, monitors, and controls device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices.

Supplemental Guidance: Portable and mobile devices (e.g., notebook computers, workstations, personal digital assistants) are ~~not~~ only allowed access to organizational networks ~~without first meeting~~ in accordance with organizational security policies and procedures. Security policies and procedures ~~might~~ should include ~~such activities as~~ device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), configuration management, scanning ~~the~~ devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared).

Control Enhancements:

(1) The organization employs ~~removable hard drives or~~ cryptography to protect information residing on portable and mobile devices.

LOW Not Selected	**MOD** AC-19 (1)	**HIGH** AC-19 (1)

AC-20 ~~PERSONALLY OWNED~~ USE OF EXTERNAL INFORMATION SYSTEMS

Control: The organization restricts the use of ~~personally owned~~ external information systems by authorized individuals ~~for~~ conducting official U.S. Government business involving the processing, storage, or transmission of federal information.

Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the organization (i.e., information systems or components for which the organization typically has no direct control over the application of required security controls), and that are used to process, store, or transmit federal information. External information systems include, but are not limited to, personally-owned information systems (e.g., laptop computers, cellular telephones, or personal digital assistants); privately-owned workstations and computing devices resident in hotels, convention centers, or airports; contractor-owned information systems; information systems owned or controlled by non-federal governmental organizations; and federal information systems that are not owned by, operated by, or under the direct control of the organization. Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational systems and information intended for public access (e.g., citizens accessing federal information through public interfaces to organizational information systems). The organization establishes strict terms and conditions for the use of ~~personally owned~~ external information systems ~~when accessing federal information and information systems. The terms and conditions should address~~ in accordance with organizational security policies and procedures. ~~at a minimum: (i) the types of applications that can be accessed from personally owned the external information systems; (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; (iii) how other users of the personally owned information system or individuals with potential access to the information system, are prevented from accessing federal information; (iv) the use of virtual private networking (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the use of adequate physical security controls; (vii) the use of malicious code protection software; (viii) how often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, virus definitions, firewall version updates, spyware definitions); and (ix) any other technologies, the application of which, may result in vulnerabilities causing potential comprise of federal information.~~

Control Enhancements: ~~None.~~

(1) **The organization prohibits information system access by authorized individuals using external information systems except in situations where the organization can verify the employment of required security controls on those external systems as specified in the organization's information security policy and information system security plan.**

(2) **The organization prohibits information system access by organizational personnel and other authorized individuals using external information systems except in formally authorized cases of operational necessity.**

LOW AC-20	**MOD** AC-20 (1)	**HIGH** AC-20 (1) (2)

FAMILY: AWARENESS AND TRAINING **CLASS:** OPERATIONAL

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

Supplemental Guidance: The security awareness and training policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-16 and 800-50 provide guidance on security awareness and training. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW AT-1	**MOD** AT-1	**HIGH** AT-1

AT-2 SECURITY AWARENESS

Control: The organization ensures that all users (including managers and senior executives) ~~are exposed to~~ receive basic information system security awareness ~~materials~~ training before authorizing access to the system, when required by system changes, and [*Assignment: organization-defined frequency, at least annually*] thereafter.

Supplemental Guidance: The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in 5 C.F.R. Part 930.301 and with the guidance in NIST Special Publication 800-50.

Control Enhancements: None.

LOW AT-2	**MOD** AT-2	**HIGH** AT-2

AT-3 SECURITY TRAINING

Control: The organization identifies personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides appropriate information system security training before authorizing access to the system, when required by system changes, and [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: The organization determines the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization ensures system managers, system and network administrators, and other personnel having access to system-level software have adequate technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in 5 C.F.R. Part 930.301 and with the guidance in NIST Special Publication 800-50.

Control Enhancements: None.

LOW AT-3	**MOD** AT-3	**HIGH** AT-3

AT-4 SECURITY TRAINING RECORDS

Control: The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.

Supplemental Guidance: None.

Control Enhancements: None.

LOW AT-4	**MOD** AT-4	**HIGH** AT-4

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

Control: The organization establishes and maintains contacts with special interest groups, specialized forums, or professional associations to stay up to date with the latest recommended security practices, techniques, and technologies.

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Supplemental Guidance: The audit and accountability policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW AU-1	**MOD** AU-1	**HIGH** AU-1

AU-2 AUDITABLE EVENTS

Control: The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*].

Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverse the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function should coordinate with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The information system provides the capability to compile audit records from multiple components throughout the system into a systemwide (logical or physical), time-correlated audit trail.

(2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.

(3) The organization periodically reviews and updates the list of organization-defined auditable events.

LOW AU-2	**MOD** AU-2 (3)	**HIGH** AU-2 (1) (2) (3)

AU-3 CONTENT OF AUDIT RECORDS

Control: Audit records produced by or associated with ~~T~~the information system ~~captures~~ contain sufficient information ~~in audit records~~ to establish what events occurred, the sources of the events, and the outcomes of the events.

Supplemental Guidance: Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event. NIST Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

(2) The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.

LOW AU-3	**MOD** AU-3 (1)	**HIGH** AU-3 (1) (2)

AU-4 AUDIT STORAGE CAPACITY

Control: The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.

Supplemental Guidance: ~~None.~~ The organization ensures that sufficient audit storage capacity is implemented, taking into account the auditing to be performed (See security control AU-2) and the online audit processing requirements (See security controls AU-6, AU-7, and SI-4).

Control Enhancements: None.

LOW AU-4	**MOD** AU-4	**HIGH** AU-4

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: In the event of an audit processing failure (e.g., software/hardware error, failure in the audit capturing mechanism, or audit storage capacity being reached), the information system alerts appropriate organizational officials and takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: None.

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage of maximum audit record storage capacity*].

(2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

LOW AU-5	**MOD** AU-5	**HIGH** AU-5 (1) (2)

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: ~~None.~~ Organizations should increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Control: The information system provides an audit reduction and report generation capability.

Supplemental Guidance: Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.

Control Enhancements:

(1) The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.

LOW Not Selected	**MOD** AU-7 (1)	**HIGH** AU-7 (1)

AU-8 TIME STAMPS

Control: The information system provides time stamps for use in audit record generation.

Supplemental Guidance: Time stamps of audit records are generated using internal system clocks ~~that are synchronized system wide~~.

Control Enhancements: ~~None.~~

(1) The organization synchronizes internal information system clocks [*Assignment: organization-defined frequency*].

LOW ~~Not Selected~~ AU-8	**MOD** AU-8 (1)	**HIGH** AU-8 (1)

AU-9 PROTECTION OF AUDIT INFORMATION

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance: None.

Control Enhancements:

(1) The information system produces audit information on hardware-enforced, write-once media.

LOW AU-9	**MOD** AU-9	**HIGH** AU-9

AU-10 NON-REPUDIATION

Control: The information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).

Supplemental Guidance: Non-repudiation protects against later false claims by an individual of not having taken a specific action. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts, time stamps).

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AU-11 AUDIT RECORD RETENTION

Control: The organization retains audit ~~logs~~ records for [*Assignment: organization-defined time period*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance: The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. NIST Special Publication 800-61 provides guidance on computer security incident handling and audit ~~log~~ record retention.

Control Enhancements: None.

LOW AU-11	**MOD** AU-11	**HIGH** AU-11

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS **CLASS:** MANAGEMENT

CA-1 CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICIES AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.

Supplemental Guidance: The security assessment and certification and accreditation policies and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The security assessment and certification and accreditation policies can be included as part of the general information security policy for the organization. Security assessment and certification and accreditation procedures can be developed for the security program in general, and for a particular information system, when required. The organization defines what constitutes a significant change to the information system to ensure security reaccreditations are conducted in a consistent manner. NIST Special Publication 800-53A provides guidance on security control assessments. NIST Special Publication 800-37 provides guidance on security certification and accreditation. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW CA-1	**MOD** CA-1	**HIGH** CA-1

CA-2 SECURITY ASSESSMENTS

Control: The organization conducts an assessment of the security controls in the information system [*Assignment: organization-defined frequency, at least annually*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Supplemental Guidance: This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be tested with a frequency depending on risk, but no less than annually. The FISMA requirement for (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place. Organizations can satisfy the FISMA requirement by using the security control assessment results from any of the following sources, including: (i) security certifications conducted as part of a routine information system accreditation or reaccreditation process; (ii) ongoing continuous monitoring activities; (iii) self assessments; or (iv) routine testing and evaluation of the information system as part of the ongoing system development life cycle process. Reuse of assessment information is critical in achieving a broad-based, cost-effective, and fully integrated security program capable of producing the needed evidence to determine the actual security status of the information system. NIST Special Publications 800-53A and 800-26 provide guidance on security control assessments.

Control Enhancements: None.

LOW Not Selected	**MOD** CA-2	**HIGH** CA-2

CA-3 INFORMATION SYSTEM CONNECTIONS

Control: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system ~~inter~~connections on an ongoing basis. Appropriate organizational officials approve information system ~~inter~~connection agreements.

Supplemental Guidance: Since FIPS 199 security categorizations apply to individual information systems, the organization should carefully consider the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations should also include information systems sharing the same networks. NIST Special Publication 800-47 provides guidance on ~~inter~~connecting information systems.

Control Enhancements: None.

LOW CA-3	**MOD** CA-3	**HIGH** CA-3

CA-4 SECURITY CERTIFICATION

Control: The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Supplemental Guidance: A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is a key factor in all authorization (accreditation) decisions and is integrated into and spans the system development life cycle. When an independent assessment is required, the certification agent (or certification team) provides an unbiased assessment of the security controls in the information system. Assessor independence implies that the certification agent (or certification team), whether obtained from within the organization or externally, is not involved with the information system's development, implementation, or operation. NIST Special Publication 800-53A provides guidance on the assessment of security controls. NIST Special Publication 800-37 provides guidance on security certification and accreditation.

Control Enhancements:

(1) The assessment of the security controls in the information system for purposes of security certification is conducted by an independent certification agent or certification team.

LOW CA-4	**MOD** CA-4 (1)	**HIGH** CA-4 (1)

CA-5 PLAN OF ACTION AND MILESTONES

Control: The organization develops and updates [*Assignment: organization-defined frequency*], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

Supplemental Guidance: The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official and is subject to federal reporting requirements established by OMB. NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems. NIST Special Publication 800-30 provides guidance on risk mitigation.

Control Enhancements: None.

LOW CA-5	**MOD** CA-5	**HIGH** CA-5

CA-6 SECURITY ACCREDITATION

Control: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [*Assignment: organization-defined frequency, at least every three years*] or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation.

Supplemental Guidance: OMB Circular A-130, Appendix III, establishes policy for security accreditations of federal information systems. The organization assesses the security controls employed within the information system before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications. NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems.

Control Enhancements: None.

LOW CA-6	**MOD** CA-6	**HIGH** CA-6

CA-7 CONTINUOUS MONITORING

Control: The organization monitors the security controls in the information system on an ongoing basis.

Supplemental Guidance: Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization establishes the selection criteria for control monitoring and subsequently selects a subset of the security controls employed within the information system for purposes of continuous monitoring. NIST Special Publication 800-37 provides guidance on the continuous monitoring process. NIST Special Publication 800-53A provides guidance on the assessment of security controls.

Control Enhancements: None.

LOW CA-7	**MOD** CA-7	**HIGH** CA-7

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Supplemental Guidance: The configuration management policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW CM-1	**MOD** CM-1	**HIGH** CM-1

CM-2 BASELINE CONFIGURATION AND SYSTEM COMPONENT INVENTORY

Control: The organization develops, documents, and maintains a current~~,~~ baseline configuration of the information system, an inventory of the system's constituent components, and relevant ownership information.

Supplemental Guidance: The configuration of the information system is consistent with the Federal Enterprise Architecture and the organization's information system architecture. The inventory of information system components includes any information deemed necessary by the organization to ensure effective property accountability (e.g., manufacturer, ~~type~~ model number, serial number, software version number, information system/component owner, ~~and location (i.e.,~~ physical location, and logical position within the information system architecture). ~~The inventory also designates those information system components required to implement and/or conduct contingency planning operations.~~

Control Enhancements:

(1) The organization updates the baseline configuration of the information system and inventory of system components as an integral part of information system component installations.

(2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system and inventory of information system components.

LOW CM-2	**MOD** CM-2 (1)	**HIGH** CM-2 (1) (2)

CM-3 CONFIGURATION CHANGE CONTROL

Control: The organization documents and controls changes to the information system. Appropriate organizational officials approve information system changes in accordance with organizational policies and procedures.

Supplemental Guidance: Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of proposed changes, including upgrades and modifications. The organization includes emergency changes in the configuration change control process. The approvals to implement a change to the information system include successful results from the security analysis of the change (See security control CM-4). The organization audits activities associated with configuration changes to the information system.

Control Enhancements:

(1) **The organization employs automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.**

LOW Not Selected	**MOD** CM-3	**HIGH** CM-3 (1)

CM-4 MONITORING CONFIGURATION CHANGES

Control: The organization monitors changes to the information system ~~and conducts~~ conducting security impact analyses to determine the effects of the changes.

Supplemental Guidance: ~~The organization documents the installation of information system components.~~ Prior to change implementation, and as part of the change approval process, the organization analyzes changes to the information system for potential security impacts. After the information system is changed (including upgrades and modifications), the organization~~s~~ checks the security features to ensure the features are still functioning properly. The organization audits activities associated with configuration changes to the information system.

Control Enhancements: None.

LOW Not Selected	**MOD** CM-4	**HIGH** CM-4

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control: The organization enforces physical and logical access restrictions associated with changes to the information system and generates, retains, and reviews records reflecting all such changes.

Supplemental Guidance: Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. Accordingly, the organization ensures that only qualified and authorized individuals obtain access to information system components for purposes of initiating changes, including upgrades, and~~/or~~ modifications. Appropriate organizational officials approve individual access privileges.

Control Enhancements:

(1) **The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.**

LOW Not Selected	**MOD** CM-5	**HIGH** CM-5 (1)

CM-6 CONFIGURATION SETTINGS

Control: The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.

Supplemental Guidance: NIST Special Publication 800-70 provides guidance on producing and using configuration settings for information technology products employed in organizational information systems.

Control Enhancements:

(1) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.

LOW CM-6	**MOD** CM-6	**HIGH** CM-6 (1)

CM-7 LEAST FUNCTIONALITY

Control: The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services*].

Supplemental Guidance: Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). The functions and services provided by information systems should be carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).

Control Enhancements:

(1) The organization reviews the information system [*Assignment: organization-defined frequency*], to identify and eliminate unnecessary functions, ports, protocols, and/or services.

LOW Not Selected	**MOD** CM-7	**HIGH** CM-7 (1)

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Supplemental Guidance: The contingency planning policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-34 provides guidance on contingency planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW CP-1	**MOD** CP-1	**HIGH** CP-1

CP-2 CONTINGENCY PLAN

Control: The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization coordinates contingency plan development with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).

(2) The organization conducts capacity planning to ensure that necessary capacity exists during crisis situations.

(3) The organization conducts impact analyses to consider the impact of the use of various services on other organizational information system requirements during crisis situations.

LOW CP-2	**MOD** CP-2 (1)	**HIGH** CP-2 (1) (2) (3)

CP-3 CONTINGENCY TRAINING

Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: None.

Control Enhancements:

(1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

LOW Not Selected	**MOD** CP-3	**HIGH** CP-3 (1)

CP-4 CONTINGENCY PLAN TESTING

Control: The organization tests the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan. Appropriate officials within the organization review the contingency plan test results and initiate corrective actions.

Supplemental Guidance: There are several methods for testing contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop exercises). The depth and rigor of contingency plan testing increases with the impact level of the information system. Contingency plan testing also includes a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) arising due to contingency operations in accordance with the plan.

Control Enhancements:

(1) The organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).

(2) The organization tests the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

(3) The organization employs automated mechanisms to more thoroughly and effectively test the contingency plan.

LOW Not Selected	**MOD** CP-4 (1)	**HIGH** CP-4 (1) (2)

CP-5 CONTINGENCY PLAN UPDATE

Control: The organization reviews the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

Supplemental Guidance: Organizational changes include changes in mission, functions, or business processes supported by the information system. The organization communicates changes to appropriate organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).

Control Enhancements: None.

LOW CP-5	**MOD** CP-5	**HIGH** CP-5

CP-6 ALTERNATE STORAGE SITES

Control: The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.

Supplemental Guidance: None.

Control Enhancements:

(1) **The alternate storage site is geographically separated from the primary storage site so as not to be susceptible to the same hazards.**

(2) **The alternate storage site is configured to facilitate timely and effective recovery operations.**

(3) **The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.**

LOW Not Selected	**MOD** CP-6 (1) (3)	**HIGH** CP-6 (1) (2) (3)

CP-7 ALTERNATE PROCESSING SITES

Control: The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [*Assignment: organization-defined time period*] when the primary processing capabilities are unavailable.

Supplemental Guidance: Equipment and supplies required to resume operations within the organization-defined time period are either available at the alternate site or contracts are in place to support delivery to the site.

Control Enhancements:

(1) **The alternate processing site is geographically separated from the primary processing site so as not to be susceptible to the same hazards.**

(2) **The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.**

(3) **Alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements.**

(4) **The alternate processing site is fully configured to support a minimum required operational capability and ready to use as the operational site.**

LOW Not Selected	**MOD** CP-7 (1) (2) (3)	**HIGH** CP-7 (1) (2) (3) (4)

CP-8 TELECOMMUNICATIONS SERVICES

Control: The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable.

Supplemental Guidance: In the event that the primary and/or alternate telecommunications services are provided by a wire line carrier, the organization should ensure that it requests Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness (See http://tsp.ncs.gov for a full explanation of the TSP program).

Control Enhancements:

(1) Primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization's availability requirements.

(2) Alternate telecommunications services do not share a single point of failure with primary telecommunications services.

(3) Alternate telecommunications service providers are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.

(4) Primary and alternate telecommunications service providers have adequate contingency plans.

LOW Not Selected	**MOD** CP-8 (1) (2)	**HIGH** CP-8 (1) (2) (3) (4)

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [*Assignment: organization-defined frequency*] and ~~stores~~ protects backup information while in transit and at ~~an appropriately secured~~ the storage location.

Supplemental Guidance: The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives.

Control Enhancements:

(1) The organization tests backup information [*Assignment: organization-defined frequency*] to ensure media reliability and information integrity.

(2) The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.

(3) The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.

(4) The organization encrypts backup information whenever the information is removed from a controlled facility and is either physically transported or electronically transmitted to another facility.

(5) The organization maintains an encrypted version of backup information.

LOW CP-9	**MOD** CP-9 (1) (4)	**HIGH** CP-9 (1) (2) (3) (4)

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to ~~the system's original~~ a known secure state after a disruption or failure.

Supplemental Guidance: ~~Secure i~~Information system recovery and reconstitution to ~~the system's original~~ a known secure state means that all system parameters (either default or organization-established) are ~~reset~~ set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is ~~available~~ loaded, and the system is fully tested.

Control Enhancements:

(1) The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.

LOW CP-10	**MOD** CP-10	**HIGH** CP-10 (1)

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Supplemental Guidance: The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and Special Publications 800-73, 800-76, and 800-78; and (ii) other applicable federal laws, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-63 provides guidance on remote electronic authentication.

Control Enhancements: None.

LOW IA-1	**MOD** IA-1	**HIGH** IA-1

IA-2 USER IDENTIFICATION AND AUTHENTICATION

Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Supplemental Guidance: Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein. FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) ~~card token~~ credential for use in the unique identification and authentication of federal employees and contractors. NIST Special Publication 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms. For other than remote situations, when users identify and authenticate to information systems within a specified security perimeter which is considered to offer sufficient protection, NIST Special Publication 800-63 guidance should be applied as follows: (i) for low-impact information systems, tokens that meet Level 1, 2, 3, or 4 requirements are acceptable; (ii) for moderate-impact information systems, tokens that meet Level 2, 3, or 4 requirements are acceptable; and (iii) for high-impact information systems, tokens that meet Level 3 or 4 requirements are acceptable. In addition to identifying and authenticating users at the information system level, identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

Control Enhancements:

(1) The information system employs multifactor authentication.

LOW IA-2	**MOD** IA-2	**HIGH** IA-2 (1)

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system identifies and authenticates specific devices before establishing a connection.

Supplemental Guidance: The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control ~~Program~~ Protocol/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is ~~based on~~ determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication.

Control Enhancements: None.

LOW Not Selected	**MOD** IA-3	**HIGH** IA-3

IA-4 IDENTIFIER MANAGEMENT

Control: The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after [*Assignment: organization-defined time period*] of inactivity; and (vi) archiving user identifiers.

Supplemental Guidance: Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) ~~card token~~ credential for use in the unique identification and authentication of federal employees and contractors.

Control Enhancements: None.

LOW IA-4	**MOD** IA-4	**HIGH** IA-4

IA-5 AUTHENTICATOR MANAGEMENT

Control: The organization manages information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and (iii) changing default authenticators upon information system installation.

Supplemental Guidance: Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the information system: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account. FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) ~~card token~~ credential for use in the unique identification and authentication of federal employees and contractors. NIST Special Publication 800-63 provides guidance on remote electronic authentication.

Control Enhancements: None.

LOW IA-5	**MOD** IA-5	**HIGH** IA-5

IA-6 AUTHENTICATOR FEEDBACK

Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance: ~~The information system may obscure feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password).~~ The feedback from the information system ~~provides sufficient information for a legitimate user to understand why access is not being granted (e.g., made a keystroke mistake, forgot the password) and, at the same time,~~ does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.

Control Enhancements: None.

LOW IA-6	**MOD** IA-6	**HIGH** IA-6

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: For authentication to a cryptographic module, the information system employs authentication methods that meet the requirements of FIPS 140-2 (as amended).

Supplemental Guidance: Where the cryptographic module is a personal identity verification (PIV) ~~card token~~ credential for use in the unique identification and authentication of federal employees and contractors, the module conforms to FIPS 201 and Special Publications 800-73 and 800-78. Module testing is in accordance with NIST Special Publication 800-85.

Control Enhancements: None.

LOW IA-7	**MOD** IA-7	**HIGH** IA-7

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Supplemental Guidance: The incident response policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-61 provides guidance on incident handling and reporting. NIST Special Publication 800-83 provides guidance on malware incident handling and prevention.

Control Enhancements: None.

LOW IR-1	**MOD** IR-1	**HIGH** IR-1

IR-2 INCIDENT RESPONSE TRAINING

Control: The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: None.

Control Enhancements:

(1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

LOW Not Selected	**MOD** IR-2	**HIGH** IR-2 (1)

IR-3 INCIDENT RESPONSE TESTING

Control: The organization tests the incident response capability for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and exercises*] to determine the incident response effectiveness and documents the results.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.

LOW Not Selected	**MOD** IR-3	**HIGH** IR-3 (1)

IR-4 INCIDENT HANDLING

Control: The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

Supplemental Guidance: Incidents include physical security incidents such as those discovered as part of monitoring physical access (see security control PE-6) and those discovered as part of audit monitoring (see security control AU-6). The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly.

Control Enhancements:

(1) The organization employs automated mechanisms to support the incident handling process.

LOW IR-4	**MOD** IR-4 (1)	**HIGH** IR-4 (1)

IR-5 INCIDENT MONITORING

Control: The organization tracks and documents information system security incidents on an ongoing basis.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

LOW Not Selected	**MOD** IR-5	**HIGH** IR-5 (1)

IR-6 INCIDENT REPORTING

Control: The organization promptly reports incident information to appropriate authorities.

Supplemental Guidance: The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. Organizational officials report cyber security incidents to the United States Computer Emergency Readiness Team (US-CERT) within the specified timeframe designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. In addition to incident information, weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents. NIST Special Publication 800-61 provides guidance on incident reporting.

Control Enhancements:

(1) The organization employs automated mechanisms to assist in the reporting of security incidents.

LOW IR-6	**MOD** IR-6 (1)	**HIGH** IR-6 (1)

IR-7 INCIDENT RESPONSE ASSISTANCE

Control: The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.

Supplemental Guidance: Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required.

Control Enhancements:

(1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.

LOW IR-7	**MOD** IR-7 (1)	**HIGH** IR-7 (1)

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

Supplemental Guidance: The information system maintenance policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW MA-1	**MOD** MA-1	**HIGH** MA-1

MA-2 PERIODIC MAINTENANCE

Control: The organization schedules, performs, and documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Supplemental Guidance: Appropriate organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks the security features to ensure that they are still functioning properly.

Control Enhancements:

(1) **The organization maintains ~~a~~ maintenance ~~log~~ records for the information system that includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).**

(2) **The organization employs automated mechanisms to ensure that periodic maintenance is scheduled and conducted as required, and that ~~a log~~ records of maintenance actions, both needed and completed, ~~is~~ are up-to date, accurate, complete, and available.**

LOW MA-2	**MOD** MA-2 (1)	**HIGH** MA-2 (1) (2)

MA-3 MAINTENANCE TOOLS

Control: The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.

Supplemental Guidance: ~~None.~~ The intent of this control is to address hardware and software brought into the information system specifically for diagnostic/repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing “ping”, “ls”, “ipconfig” or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control.

Control Enhancements:

(1) The organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.

(2) The organization checks all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system.

(3) The organization checks all maintenance equipment with the capability of retaining information to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.

(4) The organization employs automated mechanisms to ensure that only authorized personnel use maintenance tools.

LOW Not Selected	**MOD** MA-3	**HIGH** MA-3 (1) (2) (3)

MA-4 REMOTE MAINTENANCE

Control: The organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.

Supplemental Guidance: The organization describes the use of remote diagnostic tools in the security plan for the information system. The organization maintains maintenance ~~logs~~ records for all remote maintenance, diagnostic, and service activities. Appropriate organization officials periodically review maintenance logs. Other techniques to consider for improving the security of remote maintenance include: (i) encryption and decryption of diagnostic communications; (ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST Special Publication 800-63; and (iii) remote disconnect verification. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections. If password-based authentication is used during remote maintenance, the organization changes the passwords following each remote maintenance service. For high-impact information systems, if remote diagnostic or maintenance services are required from a service or organization that does not implement for its own information system the same level of security as that implemented on the system being serviced, the system being serviced is sanitized and physically separated from other information systems before the connection of the remote access line. If the information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed.

Control Enhancements:

(1) **The organization audits all remote maintenance sessions, and appropriate organizational personnel review the ~~audit logs~~ maintenance records of the remote sessions.**

(2) **The organization addresses the installation and use of remote diagnostic links in the security plan for the information system.**

(3) **Remote diagnostic or maintenance services are acceptable if performed by ~~a service or~~ an organization that implements, for its own information system, the same level of security as that implemented on the information system being serviced.**

LOW MA-4	**MOD** MA-4	**HIGH** MA-4 (1) (2) (3)

MA-5 MAINTENANCE PERSONNEL

Control: ~~The organization maintains a list of personnel authorized to perform maintenance on the information system.~~ Only authorized personnel perform maintenance on the information system.

Supplemental Guidance: Maintenance personnel have appropriate access authorizations to the information system when maintenance activities allow access to organizational information. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.

Control Enhancements: ~~None.~~

(1) **The organization maintains a list of all personnel who are authorized to perform maintenance on the information system.**

LOW MA-5	**MOD** MA-5	**HIGH** MA-5 (1)

MA-6 TIMELY MAINTENANCE

Control: The organization obtains maintenance support and spare parts for [*Assignment: organization-defined list of key information system components*] within [*Assignment: organization-defined time period*] of failure.

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** MA-6	**HIGH** MA-6

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

Supplemental Guidance: The media protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW MP-1	**MOD** MP-1	**HIGH** MP-1

MP-2 MEDIA ACCESS

Control: The organization ensures that only authorized users have access to information in printed form or on digital media removed from the information system.

Supplemental Guidance: ~~None~~ The rigor with which this control is applied is determined by the FIPS 199 categorization of the information. For example, this control has limited applicability to printed or digital media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if accessed by other than authorized personnel. For low impact information, physical access controls to the facility where the information system and media storage areas reside provide adequate protection for this type of information and associated storage media. More rigorous application of the control is necessary for moderate and high impact information.

Control Enhancements:

(1) Unless guard stations control access to media storage areas, the organization employs automated mechanisms to ensure only authorized access to such storage areas and to audit access attempts and access granted.

LOW MP-2	**MOD** MP-2 (1)	**HIGH** MP-2 (1)

MP-3 MEDIA LABELING

Control: The organization affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information. The organization exempts the following specific types of media or hardware components from labeling so long as they remain within a secure environment: [*Assignment: organization-defined list of media types and hardware components*].

Supplemental Guidance: The organization marks human-readable output appropriately in accordance with applicable policies and procedures. At a minimum, the organization affixes printed output that is not otherwise appropriately marked, with cover sheets and labels digital media with the distribution limitations, handling caveats, and applicable security markings, if any, of the information.

Control Enhancements: None.

LOW Not Selected	**MOD** MP-3	**HIGH** MP-3

MP-4 MEDIA STORAGE

Control: The organization physically controls and securely stores information system media, both paper and digital, based on the highest FIPS 199 security category of the information recorded on the media.

Supplemental Guidance: The organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. The organization protects unmarked media at the highest FIPS 199 security category for the information system until the media are reviewed and appropriately labeled.

Control Enhancements: ~~None.~~

(1) Media are stored in locked canisters or encrypted when removed from the primary storage area.

LOW Not Selected	**MOD** MP-4 (1)	**HIGH** MP-4 (1)

MP-5 MEDIA TRANSPORT

Control: The organization controls information system media (paper and digital) during transport and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.

Supplemental Guidance: ~~None.~~ This control is applied based upon the FIPS 199 impact level of the information being transported. When that level cannot be determined, the impact level of the information system from which the information came will be used. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service) provided there are specific assurances that appropriate protection measures are in place during the media transport process.

Control Enhancements: ~~None.~~

(1) **The organization encrypts information on digital media and places non digital media in appropriately locked canisters during transport outside of organization-controlled areas.**

(2) **Media are transported under an identified custodian at all times with formal handoff of responsibility between custodians.**

Enhancement Supplemental Guidance: Organizations employ a formal system of records to document pickup, receipt, transfer, and delivery activities associated with the transport of information system media.

LOW Not Selected	**MOD** MP-5 (1)	**HIGH** MP-5 (1) (2)

MP-6 MEDIA SANITIZATION AND DISPOSAL

Control: The organization~~: (i)~~ sanitizes information system media, both paper and digital, prior to disposal or release for reuse~~; (ii) tracks, documents, and verifies media sanitization actions; and (iii) periodically tests sanitization equipment and procedures to ensure correct performance~~.

Supplemental Guidance: Sanitization is the process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, ensure that organizational information is not disclosed to unauthorized individuals when such media is reused or disposed. The organization uses its discretion on sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposed. ~~The National Security Agency provides media sanitization guidance and maintains a listing of approved sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.~~ NIST Special Publication 800-88 provides guidance on media sanitization.

Control Enhancements: ~~None.~~

(1) **The organization tracks, documents, and verifies media sanitization actions.**

(2) **The organization periodically tests sanitization equipment and procedures to ensure correct performance.**

LOW MP-6	**MOD** MP-6	**HIGH** MP-6 (1) (2)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

Supplemental Guidance: The physical and environmental protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW PE-1	**MOD** PE-1	**HIGH** PE-1

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control: The organization develops and keeps current a list~~s~~ of personnel with authorized access to the faciliti~~es~~y ~~containing~~ where the information system~~s~~ resides (except for those areas within the faciliti~~es~~y officially designated as publicly accessible) and issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: The organization promptly removes from the access list personnel no longer requiring access ~~from access lists~~ to the facility where the information system resides.

Control Enhancements: None.

LOW PE-2	**MOD** PE-2	**HIGH** PE-2

PE-3 PHYSICAL ACCESS CONTROL

Control: The organization controls all physical access points (including designated entry/exit points) to the faciliti~~es~~y ~~containing~~ where the information system~~s~~ resides (except for those areas within the faciliti~~es~~y officially designated as publicly accessible) and verifies individual access authorizations before granting access to the faciliti~~es~~y. The organization ~~also~~ controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Supplemental Guidance: The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys: (i) periodically; and (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated. ~~After an emergency-related event, the organization restricts reentry to facilities to authorized individuals only.~~ Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled. Where federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publication 800-73. If the token-based access control function employs cryptographic verification, the access control system conforms to the requirements of NIST Special Publication 800-78. If the token-based access control function employs biometric verification, the access control system conforms to the requirements of NIST Special Publication 800-76.

Control Enhancements: ~~None.~~

(1) **The organization controls physical access to the information system independent of the physical access controls for the facility.**

Enhancement Supplemental Guidance: This control enhancement in general, applies to server rooms, communications centers or any other areas within a facility containing large concentrations of information system components. It is not intended to apply to workstations or peripheral devices that are typically dispersed throughout the facility and used routinely by organization personnel.

LOW PE-3	**MOD** PE-3	**HIGH** PE-3 (1)

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities to prevent accidental damage, eavesdropping, in-transit modification, disruption, or physical tampering.

Supplemental Guidance: Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** PE-4

PE-5 ACCESS CONTROL FOR DISPLAY MEDIUM

Control: The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** PE-5	**HIGH** PE-5

PE-6 MONITORING PHYSICAL ACCESS

Control: The organization monitors physical access to the information system~~s~~ to detect and respond to physical security incidents.

Supplemental Guidance: The organization reviews physical access logs periodically~~,~~ and investigates apparent security violations or suspicious physical access activities~~, and takes remedial actions~~. Response to detected incidents is part of the organization's incident response capability.

Control Enhancements:

(1) The organization monitors real-time physical intrusion alarms and surveillance equipment.

(2) The organization employs automated mechanisms to ensure potential intrusions are recognized and appropriate response actions initiated.

LOW PE-6	**MOD** PE-6 (1)	**HIGH** PE-6 (1) (2)

PE-7 VISITOR CONTROL

Control: The organization controls physical access to the information system~~s~~ by authenticating visitors before authorizing access to the facilit~~ies~~y where the information system resides ~~or areas~~ other than areas designated as publicly accessible.

Supplemental Guidance: Government contractors and others with permanent authorization credentials are not considered visitors. Personal Identity Verification (PIV) credentials for federal ~~government~~ employees and contractors conform to FIPS 201, and the issuing organizations for the PIV credentials are accredited in accordance with the provisions of NIST Special Publication 800-79.

Control Enhancements:

(1) The organization escorts visitors and monitors visitor activity, when required.

LOW PE-7	**MOD** PE-7 (1)	**HIGH** PE-7 (1)

PE-8 ACCESS ~~LOGS~~ RECORDS

Control: The organization maintains ~~a~~ visitor access ~~log~~ records to the facilit~~ies~~y where the information system resides (except for those areas within the facilit~~ies~~y officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access ~~logs~~ records [*Assignment: organization-defined frequency*].

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the maintenance and review of access ~~logs~~ records.

(2) The organization maintains a record of all physical access, both visitor and authorized individuals.

LOW PE-8	**MOD** PE-8	**HIGH** PE-8 (1) (2)

PE-9 POWER EQUIPMENT AND POWER CABLING

Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs redundant and parallel power cabling paths.

LOW Not Selected	**MOD** PE-9	**HIGH** PE-9

PE-10 EMERGENCY SHUTOFF

Control: For specific locations within a facility containing concentrations of information system resources ~~(e.g., data centers, server rooms, mainframe rooms)~~, the organization provides the capability of shutting off power to any information ~~technology~~ system component that may be malfunctioning ~~(e.g., due to an electrical fire)~~ or threatened ~~(e.g., due to a water leak)~~ without endangering personnel by requiring them to approach the equipment.

Supplemental Guidance: ~~None.~~ Facilities containing concentrations of information system resources may include, for example, data centers, server rooms, and mainframe rooms.

Control Enhancements: ~~None.~~

(1) The emergency power-off capability is protected from accidental and intentional/unauthorized activation.

LOW Not Selected	**MOD** PE-10	**HIGH** PE-10 (1)

PE-11 EMERGENCY POWER

Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

Supplemental Guidance: None.

Control Enhancements:

(1) **The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.**

(2) **The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.**

LOW Not Selected	**MOD** PE-11	**HIGH** PE-11 (1)

PE-12 EMERGENCY LIGHTING

Control: The organization employs and maintains automatic emergency lighting ~~systems~~ that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.

Supplemental Guidance: None.

Control Enhancements: None.

LOW PE-12	**MOD** PE-12	**HIGH** PE-12

PE-13 FIRE PROTECTION

Control: The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.

Supplemental Guidance: Fire suppression and detection devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Control Enhancements:

(1) **Fire ~~suppression and~~ detection devices/systems activate automatically and notify the organization and emergency responders in the event of a fire.**

(2) **Fire suppression ~~and detection~~ devices/systems provide automatic notification of any activation to the organization and emergency responders.**

(3) **Facilities that are not manned on a continuous basis include an automatic fire suppression capability.**

LOW PE-13	**MOD** PE-13 (1) (2) (3)	**HIGH** PE-13 (1) (2) (3)

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: The organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facilit~~ies~~y ~~containing~~ where the information system~~s~~ resides.

Supplemental Guidance: None.

Control Enhancements: None.

LOW PE-14	**MOD** PE-14	**HIGH** PE-14

PE-15 WATER DAMAGE PROTECTION

Control: The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs ~~automated~~ mechanisms to ~~automatically close shutoff valves~~ prevent, without manual intervention, water damage in the event of a significant water leak.

LOW PE-15	**MOD** PE-15	**HIGH** PE-15 (1)

PE-16 DELIVERY AND REMOVAL

Control: The organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items.

Supplemental Guidance: The organization controls delivery areas and, if possible, isolates the areas from the information system and media libraries to avoid unauthorized access. Appropriate organizational officials authorize the delivery or removal of information system-related items belonging to the organization.

Control Enhancements: None.

LOW PE-16	**MOD** PE-16	**HIGH** PE-16

PE-17 ALTERNATE WORK SITE

Control: Individuals within the organization employ appropriate information system security controls at alternate work sites.

Supplemental Guidance: NIST Special Publication 800-46 provides guidance on security in telecommuting and broadband communications. The organization provides a means for employees to communicate with information system security staff in case of security problems.

Control Enhancements: None.

LOW Not Selected	**MOD** PE-17	**HIGH** PE-17

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation~~, eating and drinking within proximity~~. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards.

Control Enhancements: ~~None.~~

(1) The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

LOW Not Selected	**MOD** PE-18	**HIGH** PE-18 (1)

PE-19 INFORMATION LEAKAGE

Control: The organization protects the information system from information leakage due to electromagnetic signals emanations.

Supplemental Guidance: The FIPS 199 security categorization (for confidentiality) of the information system and organizational security policy guides the application of safeguards and countermeasures employed to protect the information system against information leakage due to electromagnetic signals emanations.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: PLANNING **CLASS:** MANAGEMENT

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

Supplemental Guidance: The security planning policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The security planning policy can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-18 provides guidance on security planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW PL-1	**MOD** PL-1	**HIGH** PL-1

PL-2 SYSTEM SECURITY PLAN

Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.

Supplemental Guidance: The security plan is aligned with the organization's information system architecture and information security architecture. NIST Special Publication 800-18 provides guidance on security planning.

Control Enhancements: None.

LOW PL-2	**MOD** PL-2	**HIGH** PL-2

PL-3 SYSTEM SECURITY PLAN UPDATE

Control: The organization reviews the security plan for the information system [*Assignment: organization-defined frequency*] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.

Supplemental Guidance: Significant changes are defined in advance by the organization and identified in the configuration management process. NIST Special Publication 800-18 provides guidance on security plan updates.

Control Enhancements: None.

LOW PL-3	**MOD** PL-3	**HIGH** PL-3

PL-4 RULES OF BEHAVIOR

Control: The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

Supplemental Guidance: Electronic signatures are acceptable for use in acknowledging rules of behavior. NIST Special Publication 800-18 provides guidance on preparing rules of behavior.

Control Enhancements: None.

LOW PL-4	**MOD** PL-4	**HIGH** PL-4

PL-5 PRIVACY IMPACT ASSESSMENT

Control: The organization conducts a privacy impact assessment on the information system.

Supplemental Guidance: OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002. ~~Only those information systems identified and/or covered by OMB policy are required to have privacy impact assessments. NIST Special Publication 800-53 provides tailoring guidance for security control baselines to ensure that the employment of specific security controls is consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.~~

Control Enhancements: None.

LOW PL-5	**MOD** PL-5	**HIGH** PL-5

PL-6 SECURITY-RELATED ACTIVITY PLANNING

Control: The organization ensures that appropriate planning and coordination occur before conducting security-related activities affecting the information system in order to minimize the impact on organizational operations (i.e., mission, functions, image, and reputation) and organizational assets.

Supplemental Guidance: Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises.

Control Enhancements: None.

LOW Not Selected	**MOD** PL-6	**HIGH** PL-6

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Supplemental Guidance: The personnel security policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW PS-1	**MOD** PS-1	**HIGH** PS-1

PS-2 POSITION CATEGORIZATION

Control: The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations [*Assignment: organization-defined frequency*].

Supplemental Guidance: Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.

Control Enhancements: None.

LOW PS-2	**MOD** PS-2	**HIGH** PS-2

PS-3 PERSONNEL SCREENING

Control: The organization screens individuals requiring access to organizational information and information systems before authorizing access.

Supplemental Guidance: Screening is consistent with: (i) 5 CFR 731.106(a); (ii) Office of Personnel Management policy, regulations, and guidance; (iii) organizational policy, regulations, and guidance; (iv) FIPS 201 and Special Publications 800-73, 800-76, and 800-78; and (v) the criteria established for the risk designation of the assigned position.

Control Enhancements: None.

LOW PS-3	**MOD** PS-3	**HIGH** PS-3

PS-4 PERSONNEL TERMINATION

Control: When employment is terminated, the organization terminates information system access, conducts exit interviews, ensures the return of all organizational information system-related property (e.g., keys, identification cards, building passes), and ensures that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems.

Supplemental Guidance: ~~None~~ Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Control Enhancements: None.

LOW PS-4	**MOD** PS-4	**HIGH** PS-4

PS-5 PERSONNEL TRANSFER

Control: The organization reviews information systems/facilities access authorizations when ~~individuals~~ personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations).

Supplemental Guidance: None.

Control Enhancements: None.

LOW PS-5	**MOD** PS-5	**HIGH** PS-5

PS-6 ACCESS AGREEMENTS

Control: The organization completes appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements [*Assignment: organization-defined frequency*].

Supplemental Guidance: None.

Control Enhancements: None.

LOW PS-6	**MOD** PS-6	**HIGH** PS-6

PS-7 THIRD-PARTY PERSONNEL SECURITY

Control: The organization establishes personnel security requirements including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management) and monitors provider compliance to ensure adequate security.

Supplemental Guidance: The organization explicitly includes personnel security requirements in acquisition-related documents. NIST Special Publication 800-35 provides guidance on information technology security services.

Control Enhancements: None.

LOW PS-7	**MOD** PS-7	**HIGH** PS-7

PS-8 PERSONNEL SANCTIONS

Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Supplemental Guidance: The sanctions process is consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The sanctions process can be included as part of the general personnel policies and procedures for the organization.

Control Enhancements: None.

LOW PS-8	**MOD** PS-8	**HIGH** PS-8

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Supplemental Guidance: The risk assessment policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-30 provides guidance on the assessment of risk. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW RA-1	**MOD** RA-1	**HIGH** RA-1

RA-2 SECURITY CATEGORIZATION

Control: The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.

Supplemental Guidance: NIST Special Publication 800-60 provides guidance on determining the security categories of the information types resident on the information system. The organization conducts security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners.

Control Enhancements: None.

LOW RA-2	**MOD** RA-2	**HIGH** RA-2

RA-3 RISK ASSESSMENT

Control: The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).

Supplemental Guidance: Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). NIST Special Publication 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments.

Control Enhancements: None.

LOW RA-3	**MOD** RA-3	**HIGH** RA-3

RA-4 RISK ASSESSMENT UPDATE

Control: The organization updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.

Supplemental Guidance: The organization develops and documents specific criteria for what is considered significant change to the information system. NIST Special Publication 800-30 provides guidance on conducting risk assessment updates.

Control Enhancements: None.

LOW RA-4	**MOD** RA-4	**HIGH** RA-4

RA-5 VULNERABILITY SCANNING

Control: The organization scans for vulnerabilities in the information system [*Assignment: organization-defined frequency*] or when significant new vulnerabilities affecting the system are identified and reported.

Supplemental Guidance: Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code). NIST Special Publication 800-42 provides guidance on network security testing. NIST Special Publication 800-40 (Version 2) provides guidance on patch and vulnerability management.

Control Enhancements:

(1) Vulnerability scanning tools include the capability to readily update the list of information system vulnerabilities scanned.

(2) The organization updates the list of information system vulnerabilities scanned [*Assignment: organization-defined frequency*] or when significant new vulnerabilities are identified and reported.

(3) Vulnerability scanning procedures include means to ensure adequate scan coverage, both vulnerabilities checked and information system components scanned.

LOW Not Selected	**MOD** RA-5	**HIGH** RA-5 (1) (2)

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

Supplemental Guidance: The system and services acquisition policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW SA-1	**MOD** SA-1	**HIGH** SA-1

SA-2 ALLOCATION OF RESOURCES

Control: The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.

Supplemental Guidance: The organization includes the determination of security requirements for the information system in mission/business case planning and establishes a discrete line item for information system security in the organization's programming and budgeting documentation. NIST Special Publication 800-65 provides guidance on integrating security into the capital planning and investment control process.

Control Enhancements: None.

LOW SA-2	**MOD** SA-2	**HIGH** SA-2

SA-3 LIFE CYCLE SUPPORT

Control: The organization manages the information system using a system development life cycle methodology that includes information security considerations.

Supplemental Guidance: NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.

Control Enhancements: None.

LOW SA-3	**MOD** SA-3	**HIGH** SA-3

SA-4 ACQUISITIONS

Control: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk.

Supplemental Guidance:

Solicitation Documents
The solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (to include FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. NIST Special Publication 800-53 provides guidance on recommended security controls for federal information systems to meet minimum security requirements for information systems categorized in accordance with FIPS 199. NIST Special Publication 800-36 provides guidance on the selection of information security products. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.

Use of Tested, Evaluated, and Validated Products
NIST Special Publication 800-23 provides guidance on the acquisition and use of tested/evaluated information technology products.

Configuration Settings and Implementation Guidance
The information system required documentation includes security configuration settings and security implementation guidance. NIST Special Publication 800-70 provides guidance on configuration settings for information technology products.

Control Enhancements: None.

LOW SA-4	**MOD** SA-4	**HIGH** SA-4

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control: The organization ensures that adequate documentation for the information system ~~and its constituent components~~ is available, protected when required, and distributed to authorized personnel.

Supplemental Guidance: Administrator and user guides include information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features.

Control Enhancements:

(1) **The organization includes documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.**

(2) **The organization includes documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).**

LOW SA-5	**MOD** SA-5 (1)	**HIGH** SA-5 (1) (2)

SA-6 SOFTWARE USAGE RESTRICTIONS

Control: The organization complies with software usage restrictions.

Supplemental Guidance: Software and associated documentation are used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Control Enhancements: None.

LOW SA-6	**MOD** SA-6	**HIGH** SA-6

SA-7 USER INSTALLED SOFTWARE

Control: The organization enforces explicit rules governing the downloading and installation of software by users.

Supplemental Guidance: If provided the necessary privileges, users have the ability to download and install software. The organization identifies what types of software downloads and installations are permitted (e.g., updates and security patches to existing software) and what types of downloads and installations are prohibited (e.g., software that is free only for personal, not government, use). ~~The organization also restricts the use of install-on-demand software.~~

Control Enhancements: None.

LOW SA-7	**MOD** SA-7	**HIGH** SA-7

SA-8 SECURITY ~~DESIGN~~ ENGINEERING PRINCIPLES

Control: The organization designs and implements the information system using security engineering principles.

Supplemental Guidance: NIST Special Publication 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.

Control Enhancements: None.

LOW Not Selected	**MOD** SA-8	**HIGH** SA-8

SA-9 OUTSOURCED INFORMATION SYSTEM SERVICES

Control: The organization ensures that third-party providers of outsourced information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. The organization monitors security control compliance.

Supplemental Guidance: The specific intent of this control is to address the outsourcing of a job, function, or facility normally inside the organization's information system boundary. In accordance with OMB policy, an organization cannot outsource its *responsibility* for the security of its information systems. For commercial services that are considered commodity items (e.g., commercial telecommunications services, network services, managed security services, or application services), the organization, where feasible, specifies required security controls in available contractual vehicles and obtains the necessary assurances that the controls are in place and effective in their application.. When it is infeasible to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk.

Third-party providers of outsourced information system services that are subject to the provisions of FISMA ~~same information system security policies and procedures of the supported organization, and~~ must conform to the same security control and documentation requirements as would apply to the organization's internal systems. Appropriate organizational officials approve outsourcing of information system services to third-party providers (e.g., service bureaus, contractors, and other external organizations). The outsourced information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service level agreements. Service level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on the security considerations in the system development life cycle.

Control Enhancements: None.

LOW SA-9	**MOD** SA-9	**HIGH** SA-9

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Control: The information system developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.

Supplemental Guidance: ~~None.~~ This control also applies to the development actions associated with information system changes.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** SA-10

SA-11 DEVELOPER SECURITY TESTING

Control: The information system developer creates a security test and evaluation plan, implements the plan, and documents the results. ~~Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system.~~

Supplemental Guidance: Developmental security test results should only be used when no security relevant modifications of the information system have been made subsequent to developer testing and after selective verification of developer test results. Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system.

Control Enhancements: None.

LOW Not Selected	**MOD** SA-11	**HIGH** SA-11

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

Supplemental Guidance: The system and communications protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW SC-1	**MOD** SC-1	**HIGH** SC-1

SC-2 APPLICATION PARTITIONING

Control: The information system separates user functionality (including user interface services) from information system management functionality.

Supplemental Guidance: The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-2	**HIGH** SC-2

SC-3 SECURITY FUNCTION ISOLATION

Control: The information system isolates security functions from nonsecurity functions.

Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.

Control Enhancements:

(1) **The information system employs underlying hardware separation mechanisms to facilitate security function isolation.**

(2) **The information system ~~further divides the~~ isolates critical security functions ~~with the~~ (i.e., functions enforcing access and information flow control) ~~isolated and protected~~ from both nonsecurity functions and from other security functions.**

(3) **The information system minimizes the ~~amount~~ number of nonsecurity functions included within the isolation boundary containing security functions.**

(4) **The information system ~~security~~ maintains its security functions in largely independent modules that avoid unnecessary interactions between modules.**

(5) **The information system security maintains its security functions in a layered structure minimizing interactions between layers of the design.**

LOW Not Selected	**MOD** Not Selected	**HIGH** SC-3

SC-4 INFORMATION REMNANTS

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: Control of information system remnants, sometimes referred to as object reuse, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-4	**HIGH** SC-4

SC-5 DENIAL OF SERVICE PROTECTION

Control: The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*].

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, network perimeter devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy.

Control Enhancements:

(1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.

(2) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

LOW SC-5	**MOD** SC-5	**HIGH** SC-5

SC-6 RESOURCE PRIORITY

Control: The information system limits the use of resources by priority.

Supplemental Guidance: Priority protection ensures that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-7 BOUNDARY PROTECTION

Control: The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Supplemental Guidance: Any connections to the Internet, or other external networks or information systems, occur through devices known as controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels). The operational failure of the boundary protection mechanisms does not result in any unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary. Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site. Implementation of security controls associated with the use of commercial telecommunication services in support of an organization's information technology infrastructure should carefully consider the intrinsically shared nature of such services. Such services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST Special Publication 800-77 provides guidance on virtual private networks.

Control Enhancements:

(1) **The organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces. The organization prevents public access into the organization's internal networks except as appropriately mediated.**

(2) **The organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.**

(3) **The organization implements and manages a controlled interface with any outsourced telecommunication services, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.**

(4) **The information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).**

LOW SC-7	**MOD** SC-7 (1) (2) (3)	**HIGH** SC-7 (1) (2) (3) (4)

SC-8 TRANSMISSION INTEGRITY

Control: The information system protects the integrity of transmitted information.

Supplemental Guidance: The FIPS 199 security category (for integrity) of the information being transmitted should guide the decision on the use of cryptographic mechanisms. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems. NIST Special Publication 800-52 provides guidance on protecting transmission integrity using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission integrity using IPsec. NIST Special Publication 800-81 provides guidance on the Domain Name System (DNS) message authentication and integrity verification mechanisms for protection of two types of transactions (i.e., zone transfer and dynamic update).

Control Enhancements:

(1) The organization employs cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).

LOW Not Selected	**MOD** SC-8	**HIGH** SC-8 (1)

SC-9 TRANSMISSION CONFIDENTIALITY

Control: The information system protects the confidentiality of transmitted information.

Supplemental Guidance: The FIPS 199 security category (for confidentiality) of the information being transmitted should guide the decision on the use of cryptographic mechanisms. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems. NIST Special Publication 800-52 provides guidance on protecting transmission confidentiality using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission confidentiality using IPsec.

Control Enhancements:

(1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).

LOW Not Selected	**MOD** SC-9	**HIGH** SC-9 (1)

SC-10 NETWORK DISCONNECT

Control: The information system terminates a network connection at the end of a session or after [*Assignment: organization-defined time period*] of inactivity.

Supplemental Guidance: ~~None.~~ The organizations applies this control within the context of risk management that considers specific mission or operational requirements; for example, when conducting, monitoring, and controlling a long-running laboratory experiment that requires continuous use of network connections.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-10	**HIGH** SC-10

SC-11 TRUSTED PATH

Control: The information system establishes a trusted communications path between the user and the following security function~~alitys~~s of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and reauthentication*].

Supplemental Guidance: ~~None~~ A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.

Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-12	**HIGH** SC-12

SC-13 USE OF VALIDATED CRYPTOGRAPHY

Control: When cryptography is employed within the information system, the cryptography complies with applicable federal laws, directives, policies, regulations, standards, and guidance, including FIPS 140-2 (as amended) which requires the system to perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.

Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management. Cryptographic module validation certificates issued by the Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2 and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked.

Control Enhancements: None.

LOW SC-13	**MOD** SC-13	**HIGH** SC-13

SC-14 PUBLIC ACCESS PROTECTIONS

Control: For publicly available information and applications ~~systems~~, the information system protects the integrity and availability of the information and applications.

Supplemental Guidance: None.

Control Enhancements: None.

LOW SC-14	**MOD** SC-14	**HIGH** SC-14

SC-15 COLLABORATIVE COMPUTING

Control: The information system prohibits remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provides an explicit indication of use to the local users (e.g., use of camera or microphone).

Supplemental Guidance: None.

Control Enhancements:

(1) The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.

LOW Not Selected	**MOD** SC-15	**HIGH** SC-15

SC-16 TRANSMISSION OF SECURITY PARAMETERS

Control: The information system reliably associates security parameters (e.g., security labels and markings) with information exchanged between information systems.

Supplemental Guidance: Security parameters may be explicitly or implicitly associated with the information contained within the information system.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: The organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.

Supplemental Guidance: The certificate policy and certification practice statement may reference in whole or in part the certificate policy and certification practice statement of the certificate issuer. Registration to receive a public key certificate includes authorization by a supervisor or a responsible official, and is done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party. NIST Special Publication 800-32 provides guidance on public key technology. NIST Special Publication 800-63 provides guidance on remote electronic authentication.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-17	**HIGH** SC-17

SC-18 MOBILE CODE

Control: The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of mobile code within the information system. Appropriate organizational officials authorize the use of mobile code.

Supplemental Guidance: Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST Special Publication 800-28 provides guidance on active content and mobile code. ~~Additional information on risk-based approaches for the implementation of mobile code technologies can be found at: http://iase.disa.mil/mcp/index.html.~~

Control Enhancements: None.

LOW Not Selected	**MOD** SC-18	**HIGH** SC-18

SC-19 VOICE OVER INTERNET PROTOCOL

Control: The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of VoIP within the information system. Appropriate organizational officials authorize the use of VoIP.

Supplemental Guidance: NIST Special Publication 800-58 provides guidance on security considerations for VoIP technologies employed in information systems.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-19	**HIGH** SC-19

SC-20 SECURE NAME ~~LOOKUP~~ /ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control: The information system (i.e., authoritative domain name system (DNS) server~~s~~) that provides ~~the~~ name ~~lookup~~ /address resolution service ~~for accessing organizational information resources to entities across the Internet~~ provides additional artifacts ~~for data origin authentication and data integrity to enable users to obtain message authentication and message integrity assurances for the information received during network-based transactions~~ (i.e., digital signatures and cryptographic keys) along with the authoritative DNS resource records it returns in response to resolution queries.

Supplemental Guidance: This control enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. NIST Special Publication 800-81 provides guidance on secure domain name system deployment.

Control Enhancements:

(1) ~~**The information system verifies the authenticity of the artifacts for data origin authentication and data integrity (i.e., public key) of any subsidiary (child) zone in the name space in instances where the subsidiary (child) zone possesses this capability (i.e., provides these artifacts).**~~ **The information system provides special types of resource records (i.e., delegation signor resource records) that serve as the authenticator for the security status of one or more child zones of the parent zone represented by the information system (if the authoritative DNS server of the child zone also provides this control).**

LOW Not Selected	**MOD** SC-20	**HIGH** SC-20

SC-21 SECURE NAME ~~LOOKUP~~ /ADDRESS RESOLUTION SERVICE (~~RESOLUTION~~ RECURSIVE OR CACHING RESOLVER)

Control: The information system (i.e., ~~authoritative domain name servers~~ resolving or caching name server) that provides ~~the~~ name ~~lookup~~ /address resolution service for ~~accessing information resources to entities within the organization~~ local clients ~~provides mechanisms for~~ performs data origin authentication and data integrity verification ~~and performs these services when requested by client systems~~ on the resolution responses it receives from authoritative domain name system (DNS) servers when requested by client systems.

Supplemental Guidance: NIST Special Publication 800-81 provides guidance on secure domain name system deployment.

Control Enhancements:

(1) **The information system performs data origin authentication and data integrity verification ~~for all information received whether or not client systems issue such requests~~ on all resolution responses whether or not local DNS clients (i.e., stub resolvers) explicitly request this function.**

LOW Not Selected	**MOD** Not Selected	**HIGH** SC-21

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

Control: The information systems that collectively provide name/address resolution service for an organization have fault tolerance and role separation.

Supplemental Guidance: To eliminate single points of failure and to ensure redundancy, there are at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. The two servers are located in two different network subnets and geographically separated (i.e., not located in the same physical facility). If organizational information technology resources are divided into those resources belonging to internal networks and external networks, authoritative DNS servers with two roles (internal and external) are established. The DNS server with the internal role provides name/address resolution information pertaining to both internal and external information technology resources while the DNS server with the external role only provides name/address resolution information pertaining to external information technology resources. The list of clients who can access the authoritative DNS server of a particular role is also specified. NIST Special Publication 800-81 provides guidance on secure DNS deployment.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-22	**HIGH** SC-22

SC-23 SESSION AUTHENTICITY

Control: The information system provides mechanisms to protect the authenticity of communications sessions.

Supplemental Guidance: This control focuses on communications protection at the session, versus packet, level. The intent of this control is to ensure that session-level protection is implemented where needed, for example, for service oriented architectures providing web-based services. NIST Special Publication 800-52 provides guidance on the use of transport layer security (TLS) mechanisms. NIST Special Publication 800-77 provides guidance on the deployment of IPsec virtual private networks (VPNs) and other methods of protecting communications sessions.

Control Enhancements:

(1) The information system implements session-level protection using FIPS 140-2 (as amended) approved cryptographic modules.

LOW Not Selected	**MOD** SC-23	**HIGH** SC-23 (1)

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

Supplemental Guidance: The system and information integrity policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW SI-1	**MOD** SI-1	**HIGH** SI-1

SI-2 FLAW REMEDIATION

Control: The organization identifies, reports, and corrects information system flaws.

Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). ~~Proprietary software can be found in either commercial/government off-the-shelf information technology component products or in custom-developed applications.~~ The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring (see security controls CA-2, CA-4, or CA-7), or incident response activities (see security control IR-4) should also be addressed expeditiously. NIST Special Publication 800-40 (Version 2), provides guidance on security patch installation and patch management.

Control Enhancements:

(1) The organization centrally manages the flaw remediation process and installs updates automatically ~~without individual user intervention~~.

(2) The organization employs automated mechanisms to periodically and upon ~~command~~ demand determine the state of information system components with regard to flaw remediation.

LOW SI-2	**MOD** SI-2 (2)	**HIGH** SI-2 (1) (2)

SI-3 MALICIOUS CODE PROTECTION

Control: The information system implements malicious code protection that includes a capability for automatic updates.

Supplemental Guidance: The organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., diskettes or compact disks), or other common means; or (ii) by exploiting information system vulnerabilities. The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. Consideration is given to using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). NIST Special Publication 800-83 provides guidance on implementing malicious code protection.

Control Enhancements:

(1) The organization centrally manages malicious code protection mechanisms.

(2) The information system automatically updates malicious code protection mechanisms.

LOW SI-3	**MOD** SI-3 (1)	**HIGH** SI-3 (1) (2)

SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES

Control: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.

Supplemental Guidance: Information system monitoring capability can be achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, ~~log~~ audit record monitoring software, network monitoring software, network forensic analysis tools). Monitoring devices can be strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices can also be deployed at ad hoc locations within the system to track specific transactions (see ~~related~~ security control AC-8 for system use notification). Additionally, these devices can be used to track the impact of security changes to the information system. The granularity of the information collected can be determined by the organization based upon its monitoring objectives and the capability of the information system to support such activities. Organizations should heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. NIST Special Publication 800-61 provides guidance on detecting attacks through various types of security technologies. NIST Special Publication 800-83 provides guidance on detecting malware-based attacks through malicious code protection software.

Control Enhancements:

(1) **The organization networks individual intrusion detection tools into a systemwide intrusion detection system using common protocols.**

(2) **The organization employs automated tools to support near-real-time analysis of events ~~in support of detecting system-level attacks~~.**

(3) **The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.**

(4) **The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions ~~indicating~~ (e.g., the presence of ~~malware, (e.g.,~~ malicious code, ~~spyware, adware)~~ the unauthorized export of data, or signaling to an external information system).**

(5) **The information system provides a real-time alert when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined list of compromise indicators*].**

LOW Not Selected	**MOD** SI-4 (4)	**HIGH** SI-4 (2) (4) (5)

SI-5 SECURITY ALERTS AND ADVISORIES

Control: The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.

Supplemental Guidance: The organization documents the types of actions to be taken in response to security alerts/advisories. The organization also maintains contact with special interest groups (e.g., information security forums) that: (i) facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies); (ii) provide access to advice from security professionals; and (iii) improve knowledge of security best practices. NIST Special Publication 800-40 provides guidance on monitoring and distributing security alerts and advisories.

Control Enhancements:

(1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

LOW SI-5	**MOD** SI-5	**HIGH** SI-5 (1)

SI-6 SECURITY FUNCTIONALITY VERIFICATION

Control: The information system verifies~~, to the extent feasible,~~ the correct operation of security functions [*Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every* [*Assignment: organization-defined time-period*]] and [*Selection (one or more): notifies system administrator, shuts the system down, restarts the system*] when anomalies are discovered.

Supplemental Guidance: ~~None.~~ The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required.

Control Enhancements:

(1) The organization employs automated mechanisms to provide notification of failed security tests.

(2) The organization employs automated mechanisms to support management of distributed security testing.

LOW Not Selected	**MOD** Not Selected	**HIGH** SI-6

SI-7 SOFTWARE AND INFORMATION INTEGRITY

Control: The information system detects and protects against unauthorized changes to software and information.

Supplemental Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** SI-7

SI-8 SPAM PROTECTION

Control: The information system implements spam protection.

Supplemental Guidance: The organization employs spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet accesses, or other common means. Consideration is given to using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). NIST Special Publication 800-45 provides guidance on electronic mail security.

Control Enhancements:

(1) The organization centrally manages spam protection mechanisms.

(2) The information system automatically updates spam protection mechanisms.

LOW Not Selected	**MOD** SI-8	**HIGH** SI-8 (1)

SI-9 INFORMATION INPUT RESTRICTIONS

Control: The organization restricts the information input to the information system to authorized personnel only.

Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Control Enhancements: None.

LOW Not Selected	**MOD** SI-9	**HIGH** SI-9

SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY

Control: The information system checks information for accuracy, completeness, validity, and authenticity.

Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information should be accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to ensure that inputs match specified definitions for format and content. Inputs passed to interpreters should be prescreened to ensure the content is not unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information should be guided by organizational policy and operational requirements.

Control Enhancements: None.

LOW Not Selected	**MOD** SI-10	**HIGH** SI-10

SI-11 ERROR HANDLING

Control: The information system identifies and handles error conditions in an expeditious manner.

Supplemental Guidance: The structure and content of error messages should be carefully considered by the organization. User error messages generated by the information system should provide timely and useful information to users without revealing information that could be exploited by adversaries. System error messages should be revealed only to authorized personnel (e.g., systems administrators, maintenance personnel). Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) should not be listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions should be guided by organizational policy and operational requirements.

Control Enhancements: None.

LOW Not Selected	**MOD** SI-11	**HIGH** SI-11

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

Control: The organization handles and retains output from the information system in accordance with organizational policy and operational requirements.

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** SI-12	**HIGH** SI-12

APPENDIX G

SECURITY CONTROL MAPPINGS

RELATIONSHIP OF SECURITY CONTROLS TO OTHER STANDARDS AND CONTROL SETS

The mapping table in this appendix provides organizations with a *general* indication of Special Publication 800-53 security control coverage with respect to other frequently referenced security control standards and control sets.[44] The security control mappings are not exhaustive and are based on a broad interpretation and general understanding of the control sets being compared. The mappings are created by using the primary security topic identified in each of the Special Publication 800-53 security controls and associated control enhancements (if any) and searching for a similar security topic in the other referenced security control standards and control sets. Security controls with similar functional meaning are included in the mapping table. For example, Special Publication 800-53 contingency planning and ISO/IEC 17799 business continuity were deemed to have similar, but not exactly the same, functionality. In some instances, similar topics are addressed in the security control sets but provide a different context, perspective, or scope. For example, Special Publication 800-53 addresses information flow broadly in terms of assigned authorizations for controlling access between source and destination objects, whereas ISO/IEC 17799 addresses the information flow more narrowly as it applies to interconnected network domains. And finally, the following cautionary notes are in order:

- The granularity of the security control~~s~~ sets being compared is not always the same. This difference in granularity makes the security control mappings less precise in some instances. Therefore, the mappings should not be used as a “checklist” for the express purpose of comparing security capabilities or security implementations across information systems assessed against different control sets.
- Some of the control sets referenced in this appendix (e.g., Department of Defense Instruction 8500.2) are organized into groups of security controls with each group reflecting different levels of protection. When the security control groups reflect a hierarchical enhancement of another group, only the paragraph reference from the lowest hierarchical group where the security topic first occurred is listed in the mapping column.

Organizations are encouraged to use the mapping table only as a starting point for conducting further analyses and interpretation of control similarity and associated coverage when comparing disparate control sets.

[44] The security control mapping table includes references to: (i) ISO/IEC 17799: June 2005, *Code of Practice for Information Security Management*; (ii) NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*; (iii) GAO, *Federal Information System Controls Audit Manual*; (iv) Director of Central Intelligence Directive 6/3 Policy and Manual, *Protecting Sensitive Compartmented Information within Information Systems*; and (v) Department of Defense Instruction 8500.2, *Information Assurance Implementation*. The designations in the respective columns indicate the paragraph identifier(s) or number(s) in the above documents where the security controls, control objectives, or associated implementation guidance may be found.

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[45]
Access Control						

AC-1	Access Control Policy and Procedures	11.1.1
		11.4.1
		15.1.1
			15.
			16.
				---	ECAN-1
					ECPA-1
					PRAS-1
					DCAR-1
						2.B.4.e(5)
						4.B.1.a(1)(b)

AC-2	Account Management	6.2.2 6.2.3 8.3.3 11.2.1 11.2.2 11.2.4 11.7.2	6.1.8 15.1.1 15.1.4 15.1.5 15.1.8 15.2.2 16.1.3 16.1.5 16.2.12	AC-2.1 AC-2.2 AC-3.2 SP-4.1	IAAC-1	4.B.2.a(3)
AC-3	Access Enforcement	11.2.4 11.4.5	10.1.2 15.1.1 16.1.1 16.1.2 16.1.3 16.1.7 16.1.9 16.2.1 16.2.7 16.2.10 16.2.11 16.2.15	AC-2 AC-3.2	DCFA-1 ECAN-1 EBRU-1 PRNK-1 ECCD-1 ECSD-2	Discretionary Access Control (DAC): 4.B.2.a(2) Mandatory Access Control (MAC): 4.B.4.a(3)
AC-4	Information Flow Enforcement	10.6.2 11.4.5 11.4.6 11.4.7	---	---	EBBD-1 EBBD-2	4.B.3.a(3) 7.B.3.g
AC-5	Separation of Duties	10.1.3 10.6.1 10.10.1	6.1.1 6.1.2 6.1.3 15.2.1 16.1.2 17.1.5	AC-3.2 SD-1.2	ECLP-1	2.A.1 4.B.3.a(18)
AC-6	Least Privilege	11.2.2	16.1.2 16.1.3 17.1.5	AC-3.2	ECLP-1	4.B.2.a(10)
AC-7	Unsuccessful Login Attempts	11.5.1	15.1.14	AC-3.2	ECLO-1	4.B.2.a(17)(c)-(d)
AC-8	System Use Notification	11.5.1 15.1.5	~~12.1.4~~ 16.2.13 16.3.1 17.1.9	AC-3.2	ECWM-1	4.B.1.a(6)

[45] References in this column are to both DCI Directive 6/3 and to its Manual (Administrative update, December 2003). Paragraphs cited from the Directive are preceded by "DCID" and where there are also references for the same control from the Manual, these are preceded by "Manual." Where only paragraph numbers appear, they are references to the Manual. References to paragraphs in the Manual should be construed to encompass all subparagraphs related to those paragraphs. It should also be noted that Special Publication 800-53 contains a set of security controls that cover personnel, physical, and technical security measures, and therefore, the scope of the publication is broader than DCID 6/3. Some of the controls in Special Publication 800-53 are explicitly not included in DCID 6/3 because they are addressed in other DCID and Intelligence Community (IC) policy documents. The difference in scope/breadth between Special Publication 800-53 and DCID 6/3 impacts the degree of correlation between the two documents. Thus, the lack of a "mapping" for a particular Special Publication 800-53 control to a DCID 6/3 requirement does not mean that there is no similar IC requirement. The IC Translation Review Board provided information for the DCID 6/3 mapping.

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[45]
AC-9	Previous Logon Notification	11.5.1	---	AC-3.2	ECLO-2	---
AC-10	Concurrent Session Control	---	---	---	ECLO-1	4.B.2.a(17)(a)
AC-11	Session Lock	11.3.2	16.1.4	AC-3.2	PESL-1	4.B.1.a(5)
AC-12	Session Termination	11.3.2 11.5.5	16.1.4 16.2.6	AC-3.2	---	4.B.2.a(17)(b)
AC-13	Supervision and Review—Access Control	10.10.2 11.2.4	7.1.10 11.2.2 16.1.10 16.2.5 17.1.6 17.1.7	AC-4 AC-4.3 SS-2.2	ECAT-1 ECAT-2 E3.3.9	2.B.7.c 4.B.3.a(8)(b)
AC-14	Permitted Actions without Identification or Authentication	---	16.2.12	---	---	7.D.3.a
AC-15	Automated Marking	7.2.2	8.2.4 16.1.6	AC-3.2	ECML-1	4.B.2.a(11)

AC-16	Automated Labeling	7.2.2	16.1.6	AC-3.2	ECML-1	4.B.1.a(3)
						4.B.4.a(15)
						4.B.4.a(16)

AC-17	Remote Access	11.4.2
		11.4.3
		11.4.4
			16.2.4
			16.2.8
				AC-3.2	EBRP-1
					EBRU-1
						4.B.1.a(1)(b)
						4.B.3.a(11)
						7.D.2.e

AC-18	Wireless Access Restrictions	11.4.2
		11.7.1
		11.7.2
			---	---	ECCT-1
					ECWN-1
						4.B.1.a(8)
						5.B.3.a(11)

AC-19	Access Control for Portable and Mobile Systems	11.7.1	7.3.1 7.3.2	---	ECWN-1	8.B.6.c 9.G.4
AC-20	~~Personally Owned~~ Use of External Information Systems	6.1.4 9.2.5 11.7.1	10.2.13	---	---	8.B.6.c
Awareness and Training						

AT-1	Security Awareness and Training Policy and Procedures	5.1.1
		8.2.2
		15.1.1
			13.	---	PRTN-1
					DCAR-1
						DCID: B.3.c
						Manual:
						2.B.2.b(8);
						2.B.4.e(6)

AT-2	Security Awareness	6.2.3 8.2.2 10.4.1 11.7.1 13.1.1 14.1.4 15.1.4	13.1.4 13.1.5	---	PRTN-1	8.B.1
AT-3	Security Training	8.2.2 10.3.2 11.7.1 13.1.1 14.1.4	13.1 13.1.3 13.1.5	---	PRTN-1	8.B.1
AT-4	Security Training Records	---	13.1.2	---	---	8.B.1
AT-5	Contacts with Security Groups and Associations	6.1.7	---	---	---	---

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[45]
Audit and Accountability						

AU-1	Audit and Accountability Policy and Procedures	10.10
		15.1.1
			17.	---	ECAT-1
					ECTB-1
					DCAR-1
						DCID: B.2.d
						Manual:
						2.B.4.e(5);
						4.B.2.a(4)

AU-2	Auditable Events	10.10.1	17.1.1 17.1.2 17.1.4	---	ECAR-3	4.B.2.a(4)(d)

AU-3	Content of Audit Records	10.10.1
		10.10.4
			17.1.1	---	ECAR-1
					ECAR-2
					ECAR-3
					ECLC-1
						4.B.2.a(4)(a)
						4.B.2.a(5)(a)

AU-4	Audit Storage Capacity	10.10.3	---	---	---	5.B.2.a(5)(a)(1)
AU-5	Response to Audit Processing Failures	10.10.3	---	---	---	4.B.4.a(9)(d)
AU-6	Audit Monitoring, Analysis, and Reporting	10.10.2 10.10.4 13.2.1	16.2.5 17.1.7 17.1.8	AC-4.3	ECAT-1 E3.3.9	4.B.4.a(10)
AU-7	Audit Reduction and Report Generation	10.10.3	17.1.2 17.1.7	---	ECRG-1	4.B.3.a(6)
AU-8	Time Stamps	10.10.6	---	---	ECAR-1	4.B.2.a(4)(a)
AU-9	Protection of Audit Information	10.10.3 15.1.3 15.3.2	17.1.3 17.1.4	---	ECTP-1	4.B.2.a(4)(b)
AU-10	Non-repudiation	10.8.2 10.9.1 12.3.1	15.1.2 17.1.1	---	DCNR-1	5.B.3.a(8)
AU-11	Audit Record Retention	10.10.1 15.1.3	17.1.4	---	ECRR-1	4.B.2.a(4)(c)
Certification, Accreditation, and Security Assessments						
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	6.1.4 10.3.2 15.1.1	2. 4.	---	DCAR-1 DCII-1	DCID: B.3 Manual: 2.B.2.b(1)

CA-2	Security Assessments	6.1.8
		15.2.1
		15.2.2
			2.1.1
			2.1.3
			2.1.4
				SP-5.1	DCII-1
					ECMT-1
					PEPS-1
					E3.3.10
						DCID: B.2.b;
						B.3.a
						Manual:
						4.B.2.b(6);
						5.B.1.b(1);
						9.B.1;
						9.B.4

CA-3	Information System Connections	10.6.2 10.9.1 11.4.5 11.4.6 11.4.7	1.1.1 3.2.9 4.1.8 12.2.3	CC-2.1	DCID-1 EBCR-1 EBRU-1 EBPW-1 ECIC-1	9.B.3 9.D.3.c

CA-4	Security Certification	10.3.2	2.1.2
			3.2.3
			3.2.5
			3.2.6
			4.1.1
			4.1.6
			11.2.8
			12.2.5
				CC-2.1	DCAR-1
					5.7.5
						DCID: B.3
						Manual:
						4.B.3.b(8);
						9.E.2.a(2);
						9.E.2.a(3)

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[45]
CA-5	Plan of Action and Milestones	15.2.1	1.1.5 1.2.3 2.2.1 4.2.1	SP-5.1 SP-5.2	5.7.5	9.E.2.a(3)(a)
CA-6	Security Accreditation	10.3.2	3.2.7 12.2.5	---	5.7.5	DCID: B.3 Manual: 9.D.3; 9.D.4

CA-7	Continuous Monitoring	15.2.1
		15.2.2
			10.2.1	---	DCCB-1
					DCPR-1
					E3.3.9
						DCID: B.2.d;
						Manual:
						2.B.4.e(7);
						2.B.5.c(10);
						5.B.2.b(2);
						9.B.1;
						9.D.7

Configuration Management						

CM-1	Configuration Management Policy and Procedures	12.4.1
		12.5.1
		15.1.1
			---	---	DCCB-1
					DCPR-1
					DCAR-1
					E3.3.8
						DCID: B.2.a
						Manual:
						2.B.4.e(5);
						5.B.2.a(5)

CM-2	Baseline Configuration and System Component Inventory	7.1.1
		15.1.2
			1.1.1
			3.1.9
			10.2.7
			10.2.9
			12.1.4
				CC-2.3
				CC-3.1
				SS-1.2
					DCHW-1
					DCSW-1
						2.B.7.c(7)
						4.B.1.c(3)
						4.B.2.b(6)

CM-3	Configuration Change Control	10.1.2
		10.2.3
		12.4.1
		12.5.1
		12.5.2
		12.5.3
			3.1.4
			10.2.2
			10.2.3
			10.2.8
			10.2.10
			10.2.11
				SS-3.2
				CC-2.2
					DCPR-1	2.B.7.c(7)
						4.B.1.c(3)
						4.B.2.b(6)
						5.B.2.a(5)

CM-4	Monitoring Configuration Changes	10.1.2	10.2.1
			10.2.4
				SS-3.1
				SS-3.2
				CC-2.1
					DCPR-1
					E3.3.8
						2.B.7.c(7)
						4.B.1.c(3)
						5.B.2.b(2)
						8.B.8.c(7)

CM-5	Access Restrictions for Change	11.6.1	6.1.3 6.1.4 10.1.1 10.1.4 10.1.5	SD-1.1 SS-1.2 SS-2.1	DCPR-1 ECSD-2	5.B.3.a(2)(b)
CM-6	Configuration Settings	---	10.2.6 10.3.1 16.2.2 16.2.3 16.2.11	---	DCSS-1 ECSC-1 E3.3.8	4.B.2.a(10)
CM-7	Least Functionality	---	10.3.1	---	DCPP-1 ECIM-1 ECVI-1 E3.3.8	4.B.2.a(10) 7.D.2.b
Contingency Planning						

CP-1	Contingency Planning Policy and Procedures	5.1.1
		10.4.1
		14.1.1
		14.1.3
		15.1.1
			9.	---	COBR-1
					DCAR-1
						2.B.4.e(5)
						6.B.1.a(1)

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[45]
CP-2	Contingency Plan	10.3.2 10.4.1 10.8.5 14.1.3 14.1.4	4.1.4 9.1.1 9.2 9.2.1 9.2.2 9.2.3 9.2.10 12.1.8 12.2.2	SC-3.1 SC-1.1	CODP-1 COEF-1	6.B.2.b(1)
CP-3	Contingency Training	14.1.3 14.1.4	9.3.2	SC-2.3	PRTN-1	8.B.1
CP-4	Contingency Plan Testing	10.5.1 14.1.5	4.1.4 9.3.3	SC-3.1	COED-1	6.B.3.b(2)(b)
CP-5	Contingency Plan Update	14.1.3 14.1.5	9.3.1 9.3.3 10.2.12	SC-2.1 SC-3.1	DCAR-1	6.B.3.b(2)

CP-6	Alternate Storage Sites	10.5.1	9.2.4
			9.2.5
			9.2.7
			9.2.9
				SC-2.1
				SC-3.1
					CODB-2	6.B.2.a(2)
						6.B.3.a(2)(d)

CP-7	Alternate Processing Sites	14.1.4	9.1.3 9.2.4 9.2.5 9.2.7 9.2.9	SC-2.1 SC-3.1	COAS-1 COEB-1 COSP-1 COSP-2	6.B.3.a(2)(d)
CP-8	Telecommunications Services	14.1.4	---	---	---	6.B.2.a(4)
CP-9	Information System Backup	10.5.1 11.7.1	9.1.1 9.2.6 9.2.9 9.3.1 12.1.9	SC-2.1	CODB-1 CODB-2 COSW-1	6.B.1.a(2)

CP-10	Information System Recovery and Reconstitution	14.1.4	9.2.8	SC-2.1	COTR-1
					ECND-1
						4.B.1.a(4)
						6.B.1.a(1)
						6.B.2.a(3)(d)

Identification and Authentication						
IA-1	Identification and Authentication Policy and Procedures	15.1.1	11.2.3	---	IAIA-1 DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5)
IA-2	User Identification and Authentication	11.2.3 11.4.2 11.5.2	15.1	---	IAIA-1	4.B.2.a(7)
IA-3	Device Identification and Authentication	11.4.2 11.4.3 11.7.1	16.2.7	---	---	4.B.5.a(14)
IA-4	Identifier Management	11.2.3 11.5.2	15.1.1 15.2.2 15.1.8	AC-2.1 AC-3.2 SP-4.1	IAGA-1 IAIA-1	4.B.1.a(2)

IA-5	Authenticator Management	11.5.2
		11.5.3
			15.1.6
			15.1.7
			15.1.9
			15.1.10
			15.1.11
			15.1.12
			15.1.13
			16.1.3
			16.2.3
				AC-3.2	IAKM-1
					IATS-1
						4.B.2.a(7)
						4.B.3.a(11)

IA-6	Authenticator Feedback	11.5.1	---	---	---	4.B.2.a(7)(g)

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[45]
IA-7	Cryptographic Module Authentication	---	16.1.7	---	---	1.G
Incident Response						

IR-1	Incident Response Policy and Procedures	10.4.1
		13.1
		13.2.1
		15.1.1
			14.	---	VIIR-1
					DCAR-1
						DCID: B.2.c; C.4
						Manual:
						2.B.4.e(5);
						2.B.2.b(6);
						2.B.6.c(10);
						8.B.7

IR-2	Incident Response Training	13.1.1	14.1.4	SP-3.4	VIIR-1	8.B.1.b(1)(f)
						8.B.1.c(1)(e)
						8.B.1.c(2)(c)

IR-3	Incident Response Testing	14.1.5	---	---	VIIR-1	8.B.7
IR-4	Incident Handling	6.1.6 13.2.1 13.2.2	2.1.5 14.1.1 14.1.2 14.1.6	SP-3.4	VIIR-1 E3.3.9	8.B.7 9.B.2.e
IR-5	Incident Monitoring	---	14.1.3	---	VIIR-1	8.B.7.a
IR-6	Incident Reporting	6.1.6 6.2.2 6.2.3 13.1.1 13.1.2	14.1.2 14.1.3 14.2.1 14.2.2 14.2.3	---	VIIR-1 E3.3.9	8.B.7
IR-7	Incident Response Assistance	14.1.3	8.1.1 14.1.1	SP-3.4	---	8.B.7.c
Maintenance						

MA-1	System Maintenance Policy and Procedures	10.1.1
		15.1.1
			10.	---	PRMP-1
					DCAR-1
						DCID: B.2.a
						Manual:
						2.B.4.e(5);
						6.B.2.a(5)

MA-2	Periodic Maintenance	9.2.4	10.1.1 10.1.3 10.2.1	SS-3.1	---	6.B.2.a(5) 8.B.8.c

MA-3	Maintenance Tools	---	10.1.3
			11.2.4
				---	---	6.B.3.a(5)
						8.B.8.c(4)
						8.B.8.c(5)

MA-4	Remote Maintenance	11.4.4	10.1.1 17.1.1	SS-3.1	EBRP-1	8.B.8.d
MA-5	Maintenance Personnel	6.2.3 9.2.4	10.1.1 10.1.3	SS-3.1	PRMP-1	8.B.8.a
MA-6	Timely Maintenance	---	9.1.2	SC-1.2	COMS-1 COSP-1	6.B.2.a(5)
Media Protection						
MP-1	Media Protection Policy and Procedures	10.1.1 10.7 15.1.1 15.1.3	8.2	---	PESP-1 DCAR-1	DCID: B.2.a Manual: 2.B.6.c(7); 8.B.2

MP-2	Media Access	10.7.3	8.2.1
			8.2.2
			8.2.3
			8.2.6
			8.2.7
				---	PEDI-1
					PEPF-1
						2.B.9.b(4)
						4.B.1.a(1)
						4.B.1.a(7)

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[45]
MP-3	Media Labeling	7.2.2 10.7.3 10.8.2 15.1.3	8.2.5 8.2.6 10.2.9	---	ECML-1	2.B.9.b(4) 8.B.2.a 8.B.2.c

MP-4	Media Storage	10.7.1
		10.7.2
		10.7.3
		10.7.4
		15.1.3
			7.1.4
			8.2.1
			8.2.2
			8.2.9
			10.1.2
				AC-3.1	PESS-1	2.B.9.b(4)
						4.B.1.a(7)

MP-5	Media Transport	10.8.3	8.2.2 8.2.4	---	---	2.B.9.b(4)
MP-6	Media Sanitization and Disposal	9.2.6 10.7.1 10.7.2	3.2.11 3.2.12 3.2.13 8.2.8 8.2.9 8.2.10	AC-3.4	PECS-1 PEDD-1	8.B.5 2.B.9.b(4) 8.B.5.a(4) 8.B.5.d 8.B.5.e
Physical and Environmental Protection						
PE-1	Physical and Environmental Protection Policy and Procedures	15.1.1	7.		PETN-1 DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5); 8.D
PE-2	Physical Access Authorizations	9.1.2 9.1.6	7.1.1 7.1.2	AC-3.1	PECF-1	4.B.1.a(1) 8.E
PE-3	Physical Access Control	9.1.1 9.1.2 9.1.5 9.1.6 10.5.1	7.1.1 7.1.2 7.1.5 7.1.6 7.1.8	AC-3.1	PEPF-1	4.B.1.a(1) 8.D.2 8.E
PE-4	Access Control for Transmission Medium	9.2.3	7.2.2 16.2.9	---	---	8.D.2 4.B.1.a(8)
PE-5	Access Control for Display Medium	9.1.2 11.3.3	7.2.1	---	PEDI-1 PEPF-1	8.C.2.a 8.D.2
PE-6	Monitoring Physical Access	9.1.2	7.1.9	AC-4	PEPF-2	4.B.1.a(1) 8.C.2.a 8.D.2
PE-7	Visitor Control	9.1.2	7.1.7 7.1.11	AC-3.1	PEVC-1	8.C.2.a 8.D.2 8.E
PE-8	Access ~~Logs~~ Records	9.1.2	7.1.9	AC-4	PEPF-2 PEVC-1	8.C.2.a 8.D.2 8.E
PE-9	Power Equipment and Power Cabling	9.2.2 9.2.3	7.1.16	SC-2.2	---	8.D.2
PE-10	Emergency Shutoff	9.2.2	---	---	PEMS-1	8.D.2

PE-11	Emergency Power	9.2.2	7.1.18	SC-2.2	COPS-1
					COPS-2
					COPS-3
						6.B.2.a(6)
						6.B.2.a(7)

PE-12	Emergency Lighting	9.2.2	---	---	PEEL-1	8.D.2
PE-13	Fire Protection	9.1.4 9.2.1	7.1.12	SC-2.2	PEFD-1 PEFS-1	8.C.2.a 8.D.2
PE-14	Temperature and Humidity Controls	9.2.1 10.5.1 10.7.1	7.1.14 7.1.15	SC-2.2	PEHC-1 PETC-1	8.D.2

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[45]
PE-15	Water Damage Protection	9.1.4 9.2.1	7.1.17	SC-2.2	---	8.C.2.a 8.D.2
PE-16	Delivery and Removal	9.1.6 9.2.7 10.7.1	7.1.3	AC-3.1	---	8.B.5.e
PE-17	Alternate Work Site	11.7.2	---	---	EBRU-1	---
PE-18	Location of Information System Components	9.2.1	---	---	---	---
PE-19	Information Leakage	---	---	---	---	---
Planning						
PL-1	Security Planning Policy and Procedures	6.1 15.1.1	5.	---	DCAR-1 E3.4.6	DCID: B.2.a Manual: 2.B.4.e(5)

PL-2	System Security Plan	6.1	4.1.5
			5.1.1
			5.1.2
			12.2.1
				SP-2.1	DCSD-1	1.F.6
						2.B.6.c(3)
						2.B.7.c(5)
						9.E.2.a(1)(d)
						9.F.2.a
						Appendix C

PL-3	System Security Plan Update	6.1	3.2.10 5.2.1	SP-2.1	5.7.5	2.B.7.c(5)
PL-4	Rules of Behavior	7.1.3 8.1.3 15.1.5	4.1.3 13.1.1	---	PRRB-1	2.B.9.b
PL-5	Privacy Impact Assessment	15.1.4	---	---	---	DCID: B.3.a Manual: 8.B.9
PL-6	Security-Related Activity Planning	15.3.1	---	---	---	---
Personnel Security						
PS-1	Personnel Security Policy and Procedures	8.1.1 15.1.1	6.	---	PRRB-1 DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5); 8.E
PS-2	Position Categorization	8.1.2	6.1.1 6.1.2	SD-1.2	---	8.E

PS-3	Personnel Screening	8.1.2	6.2.1
			6.2.3
				SP-4.1	PRAS-1	2.B.7.c(2)
						2.B.8.b(5)
						8.E

PS-4	Personnel Termination	8.1.3
		8.3
		11.2.1
			6.1.7	SP-4.1	5.12.7	2.B.9.b(6)
						4.B.2.a(3)(e)
						8.E

PS-5	Personnel Transfer	8.3.1 8.3.3 11.2.1	6.1.7	SP-4.1	5.12.7	2.B.9.b(6)
PS-6	Access Agreements	6.1.5 8.1.3	6.1.5 6.2.2	SP-4.1	PRRB-1	1.E.2 8.E

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[45]
PS-7	Third-Party Personnel Security	6.2.1 6.2.3 8.1.1 8.1.2 8.1.3 8.2.1 8.2.2 11.2.1	---	SP-4.1	5.7.10	1.A.1 8.D 8.E
PS-8	Personnel Sanctions	8.2.3 11.2.1	6.1.5	---	PRRB-1	4.B.2.a(3)(e) 8.E
Risk Assessment						
RA-1	Risk Assessment Policy and Procedures	4.1 15.1.1	1.	---	DCAR-1	DCID: B.3.a Manual: 2.B.4.e(5)

RA-2	Security Categorization	7.2.1	1.1.3
			3.1.1
				SP-1
				AC-1.1
				AC-1.2
					E3.4.2	3.C
						3.D
						9.E.2.a(1)(a)
						9.E.2.a(1)(d)

RA-3	Risk Assessment	4.0 4.1 4.2 6.2.1 10.10.2 10.10.5 12.5.1 12.6.1 14.1.1 14.1.2	1.1.2 1.1.4 1.1.5 1.1.6 1.2.1 1.2.2 1.2.3 3.1.7 3.1.8 4.1.7 7.1.13 7.1.19 12.2.4	SP-1	DCDS-1 DCII-1 E3.3.10	9.B
RA-4	Risk Assessment Update	4.1	1.1.2 4.1.2	SP-1	DCAR-1 DCII-1	9.B.4.f 9.D.1.d

RA-5	Vulnerability Scanning	12.6.1	10.3.2
			14.2.1
				---	ECMT-1
					VIVM-1
						4.B.3.a(8)(b)
						4.B.3.b(6)(b)
						9.B.4.e

System and Services Acquisition						
SA-1	System and Services Acquisition Policy and Procedures	12.1 15.1.1	3.	---	DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5)
SA-2	Allocation of Resources	10.3.1	3.1.2 3.1.3 3.1.5 5.1.3	---	DCPB-1 E3.3.4	DCID: C.2.a Manual: 2.B.4.e(8)
SA-3	Life Cycle Support	---	3.1	---	5.8.1	DCID: B.2.a Manual: 9.E.2
SA-4	Acquisitions	12.1.1	3.1.6 3.1.7 3.1.10 3.1.11 3.1.12	---	DCAS-1 DCDS-1 DCIT-1 DCMC-1	DCID: B.2.a; C.2.a Manual: 9.B.4

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[45]

SA-5	Information System Documentation	10.7.4	3.2.3
			3.2.4
			3.2.8
			12.1.1
			12.1.2
			12.1.3
			12.1.6
			12.1.7
				CC-2.1	DCCS-1
					DCHW-1
					DCID-1
					DCSD-1
					DCSW-1
					ECND-1
					DCFA-1
						4.B.2.b(2)
						4.B.2.b(3)
						4.B.4.b(4)
						9.C.3

SA-6	Software Usage Restrictions	15.1.2	10.2.10 10.2.13	SS-3.2 SP-2.1	DCPD-1	2.B.9.b(11)
SA-7	User Installed Software	15.1.2	10.2.10	SS-3.2	---	2.B.9.b(11)
SA-8	Security ~~Design~~ Engineering Principles	12.1	3.2.1	---	DCBP-1 DCCS-1 E3.4.4	1.H.1
SA-9	Outsourced Information System Services	6.2.1 6.2.3 10.2.1 10.2.2 10.6.2	12.2.3	---	DCDS-1 DCID-1 DCIT-1 DCPP-1	1.B.1 8.C.2 8.E
SA-10	Developer Configuration Management	12.5.1 12.5.2	---	SS-3.1 C~~M~~C-3	---	4.B.4.b(4) 8.C.2.a
SA-11	Developer Security Testing	12.5.1 12.5.2	3.2.1 3.2.2 10.2.5 12.1.5	SS-3.1 C~~M~~C-~~3~~2.1	E3.4.4	4.B.4.b(4)
System and Communications Protection						
SC-1	System and Communications Protection Policy and Procedures	10.8.1 15.1.1	---	---	DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5)

SC-2	Application Partitioning	11.4.5	---	---	DCPA-1	4.B.3.b(6)(a)
						4.B.4.b(8)
						5.B.3.b(2)

SC-3	Security Function Isolation	11.4.5	---	---	DCSP-1	4.B.3.b(6)(a)
						4.B.4.b(8)
						5.B.3.b(1)
						5.B.3.b(2)

SC-4	Information Remnants	10.8.1	---	AC-3.4	ECRC-1	4.B.2.a(14)
SC-5	Denial of Service Protection	10.8.4 13.2.1	---	---	---	6.B.3.a(6)
SC-6	Resource Priority	---	---	---	---	6.B.3.a(11)
SC-7	Boundary Protection	11.4.6	16.2.2 16.2.7 16.2.9 16.2.10 16.2.11 16.2.14	AC-3.2	COEB-1 EBBD-1 ECIM-1 ECVI-1	4.B.4.a(27) 5.B.3.a(11)(b) 7.A.3 7.B 7.C 7.D
SC-8	Transmission Integrity	10.6.1 10.8.1 10.9.1	11.2.1 11.2.4 11.2.9 16.2.14	AC-3.2	ECTM-1	5.B.3.a(11)
SC-9	Transmission Confidentiality	10.6.1 10.8.1 10.9.1	---	---	ECCT-1	4.B.1.a(8)(a)
SC-10	Network Disconnect	11.5.6	16.2.6	AC-3.2	---	4.B.2.a(17)

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[45]
SC-11	Trusted Path	10.9.2	16.2.7	---	---	4.B.4.a(14)
SC-12	Cryptographic Key Establishment and Management	12.3.1 12.3.2	16.1.7 16.1.8	---	IAKM-1	1.G
SC-13	Use of Validated Cryptography	---	16.1.7 16.1.8	---	IAKM-1 IATS-1	1.G.1
SC-14	Public Access Protections	10.7.4 10.9.3	---	---	EBPW-1	---
SC-15	Collaborative Computing	---	---	---	ECVI-1	7.G
SC-16	Transmission of Security Parameters	7.2.2 10.8.2 10.9.2	16.1.6	AC-3.2	ECTM-2	4.B.1.a(3)

SC-17	Public Key Infrastructure Certificates	12.3.2	---	---	IAKM-1	2.B.4.e(5)
						4.B.3.a(11)

SC-18	Mobile Code	10.4.1 10.4.2	---	---	DCMC-1	2.B.4.e(5) 7.E
SC-19	Voice Over Internet Protocol	---	---	---	ECVI-1	---[46]
SC-20	Secure Name ~~Lookup~~ /Address Resolution Service (Authoritative Source)	---	---	---	---	---
SC-21	Secure Name ~~Lookup~~ /Address Resolution Service (~~Resolution~~ Recursive or Caching Resolver)	---	---	---	---	---
SC-22	Architecture and Provisioning for Name/Address Resolution Service	---	---	---	---	---
SC-23	Session Authenticity	---	---	---	---	---
	System and Information Integrity					

SI-1	System and Information Integrity Policy and Procedures	15.1.1	11.	---	DCAR-1	DCID: B.2.a
						Manual:
						2.B.4.e(5)
						5.B.1.b(1)
						5.B.2.a(5)(a)(1)

SI-2	Flaw Remediation	10.10.5
		12.4.1
		12.5.1
		12.5.2
		12.6.1
			10.3.2
			11.1.1
			11.1.2
			11.2.2
			11.2.7
				SS-2.2	DCSQ-1
					DCCT-1
					VIVM-1
					~~E3.3.5.7~~
						5.B.2.a(5)(a)(3)
						6.B.2.a(5)

SI-3	Malicious Code Protection	10.4.1	11.1.1
			11.1.2
				---	ECVP-1
					VIVM-1
						5.B.1.a(4)
						7.B.4.b(1)

SI-4	Information System Monitoring Tools and Techniques	10.6.2
		10.10.1
		10.10.2
		10.10.4
			11.2.5
			11.2.6
				---	EBBD-1
					EBVC-1
					ECID-1
						4.B.2.a(5)(b)
						4.B.3.a(8)(b)
						6.B.3.a(8)

SI-5	Security Alerts and Advisories	6.1.7 10.4.1	14.1.1 14.1.2 14.1.5	SP-3.4	VIVM-1	8.B.7

SI-6	Security Functionality Verification	---	11.2.1
			11.2.2
				SS-2.2	DCSS-1	4.B.1.c(2)
						5.B.2.b(2)

[46] Appropriate authorizing officials approve the use of specific technologies, including Voice Over Internet Protocol. See also DCID 6/3 paragraph 2.B.4.d and 9.D.1.a.

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[45]

SI-7	Software and Information Integrity	12.2.1
		12.2.2
		12.2.4
			11.2.1
			11.2.4
				---	ECSD-2	4.B.1.c(2)
						5.B.1.a(3)
						5.B.2.a(6)

SI-8	Spam Protection	---	---	---	---	5.B.1.a(4)
SI-9	Information Input Restrictions	12.2.1 12.2.2	---	SD-1	---	2.B.9.b(11)
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	10.7.3 12.2.1 12.2.2	---	---	---	7.B.2.h 2.B.4.d
SI-11	Error Handling	12.2.1 12.2.2 12.2.3 12.2.4	---	---	---	2.B.4.d
SI-12	Information Output Handling and Retention	10.7.3 12.2.4	---	---	PESP-1	2.B.4.d 8.B.9 8.G

APPENDIX H

STANDARDS AND GUIDANCE MAPPINGS

CROSSWALK BETWEEN NIST STANDARDS AND GUIDELINES AND SECURITY CONTROLS

The mapping table in this appendix provides organizations with a two-way crosswalk between NIST security standards and guidance documents (i.e., the current version of the FIPS Publications and Special Publications in the 800- series) and the security controls in the catalog of controls listed in Appendix F. The first crosswalk maps a specific NIST security publication to the associated security controls in NIST Special Publication 800-53 that are relevant to that publication. The second crosswalk maps each security control in Special Publication 800-53 to the appropriate NIST standards and guidance documents that apply to that particular control.[47] The purpose of the crosswalk is to provide organizations with additional useful information regarding security control selection and implementation. The two-way crosswalk between publications and security controls and security controls and publications is not intended to be exhaustive. In addition to providing useful information for organizations, the crosswalk also indicates particular areas where additional security guidance might be needed.

[47] There are certain FIPS and NIST Special Publications that are listed in the crosswalk for a particular security control in Appendix H that do not appear in the supplemental guidance for that control. The supplemental guidance for security controls lists only the most relevant NIST publications associated with that control or the publications that provide the most extensive guidance for that security control area.

CROSSWALK ONE: NIST PUBLICATION TO SECURITY CONTROLS

PUBLICATION NO.	PUBLICATION TITLE	RELATED SECURITY CONTROLS
FIPS 140-2	Security Requirements for Cryptographic Modules, May 2001	IA-7, SC-12, SC-13
FIPS 180-2	Secure Hash Standard (SHS), February 2004	SC-13
FIPS 186-2	Digital Signature Standard (DSS), October 2001	SC-13
FIPS 188	Standard Security Labels for Information Transfer, September 1994	AC-16
FIPS 190	Guideline for the Use of Advanced Authentication Technology Alternatives, September 1994	IA-1, IA-5, SC-13
FIPS 197	Advanced Encryption Standard, November 2001	SC-13
FIPS 198	The Keyed-Hash Message Authentication Code (HMAC), March 2002	AU-10, SC-8, SC-13
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems, February 2004	PL-2, RA-2
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems, March 2006	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PS-1, RA-1, SA-1, SC-1, SI-1
FIPS 201-1	Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006	AC-1, AC-3, AC-17, IA-1, IA-2, IA-4, IA-5, PL-5, SC-13, SC-17
SP 800-12	An Introduction to Computer Security: The NIST Handbook, October 1995	AC-1, AC-2, AC-3, AC-6, AC-13, AC-16, AT-1, AU-1, AU-2, AU-3, AU-6, AU-7, AU-9, CA-1, CM-1, CP-1, CP-2, CP-4, IA-1, IA-2, IR-1, MA-1, MP-1, PE-1, PE-3, PE-4, PE-13, PL-1, PL-2, PL-5, PS-1, PS-2, PS-3, PS-4, PS-5, RA-1, RA-3, RA-4, SA-1, SA-3, SC-1, SC-12, SC-13, SC-14, SI-1
SP 800-13	Telecommunications Security Guidelines for Telecommunications Management Network, October 1995	CP-8, RA-3, RA-4
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, CP-2, CP-5, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PS-1, PS-4, RA-1, RA-3, RA-4, SA-1, SA-3, SC-1, SI-1
SP 800-15	Minimum Interoperability Specification for PKI Components (MISPC), Version 1, September 1997	SC-17
SP 800-16	Information Technology Security Training Requirements: A Role- and Performance-Based Model, April 1998	AT-3
SP 800-17	Modes of Operation Validation System (MOVS): Requirements and Procedures, February 1998	CA-2, SC-13
SP 800-18, Revision 1	Guide for Developing Security Plans for Federal Information Systems, February 2006	CA-3, CA-5, PL-1, PL-2, PL-3
SP 800-19	Mobile Agent Security, October 1999	AC-1, AC-3, AC-6, AU-3, AU-9, PL-2, PL-5, RA-3, RA-4, SC-2, SI-3, SI-7

PUBLICATION NO.	PUBLICATION TITLE	RELATED SECURITY CONTROLS
SP 800-20	Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures, April 2000	CA-2, SC-13
SP 800-21-1	Second Edition, Guideline for Implementing Cryptography in the Federal Government, December 2005	CP-9, CP-10, PL-2, SA-3, SC-12, SC-13
SP 800-22	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, May 2001	CA-2, SC-13
SP 800-23	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, August 2000	CA-1, CA-2, RA-3, RA-4, SA-4
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does, August 2000	AC-17, CP-10, IA-2, MA-2, MP-6, PE-3, RA-3, RA-4, RA-5
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication, October 2000	CP-9, IA-1, IA-5, PL-2, RA-3, RA-4, SC-17
SP 800-26	Security Self-Assessment Guide for Information Technology Systems, November 2001	CA-1, CA-2, CA-7, PL-2, RA-2
SP 800-27, Revision A	Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, June 2004	PL-2, SA-3, SA-8
SP 800-28	Guidelines on Active Content and Mobile Code, October 2001	AC-6, RA-3, RA-4, SC-1, SC-7, SC-15, SC-18, SI-2
SP 800-29	A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2, June 2001	SC-13
SP 800-30	Risk Management Guide for Information Technology Systems, July 2002	CA-5, PL-2, RA-1, RA-2, RA-3, RA-4, SA-3
SP 800-31	Intrusion Detection Systems (IDS), November 2001	IR-4, PL-2, RA-3, RA-4, RA-5, SA-4, SI-1, SI-4, SI-7
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure, February 2001	IA-5, PL-2, RA-3, RA-4, SC-17, SC-20
SP 800-33	Underlying Technical Models for Information Technology Security, December 2001	PL-2, SA-8
SP 800-34	Contingency Planning Guide for Information Technology Systems, June 2002	CP-1, CP-2, CP-3, CP-4, CP-5, CP-6, CP-7, CP-8, CP-9, CP-10, MA-1, PL-2, RA-3, RA-4, SA-3
SP 800-35	Guide to Information Technology Security Services, October 2003	CA-2, CM-2, SA-1, SA-2, SA-3, SA-9
SP 800-36	Guide to Selecting Information Technology Security Products, October 2003	AC-1, CA-2, IA-1, IR-4, MP-6, RA-5, SA-1, SA-4, SC-7, SC-17, SI-3, SI-4
SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004	CA-1, CA-2, CA-4, CA-5, CA-6, CA-7, CM-1, PL-2, PL-3, RA-1, RA-2, RA-3, RA-4, RA-5

PUBLICATION NO.	PUBLICATION TITLE	RELATED SECURITY CONTROLS
SP 800-38A	Recommendation for Block Cipher Modes of Operation - Methods and Techniques, December 2001	SC-13
SP 800-38B	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005	SC-13
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, May 2004	SC-13
SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication (Draft), April 2006	SC-13
SP 800-40, Version 2	Creating a Patch and Vulnerability Management Program, November 2005	AT-3, AT-5, CM-2, CM-6, PL-2, RA-2, RA-3, RA-4, RA-5, SI-2, SI-4, SI-5
SP 800-41	Guidelines on Firewalls and Firewall Policy, January 2002	AC-1, AC-4, CP-9, PL-2, SC-7
SP 800-42	Guideline on Network Security Testing, October 2003	AU-6, CA-7, PL-1, RA-3, RA-4, RA-5, SI-3, SI-4
SP 800-43	Systems Administration Guidance for Windows 2000 Professional, November 2002	AC-2, CM-6, SI-2, CP-9, CP-10
SP 800-44	Guidelines on Securing Public Web Servers, September 2002	AC-1, AC-17, AU-1, AU-2, AU-6, AU-7, IA-2, CM-6, CP-9, CP-10, IA-1, PL-2, PL-5, RA-3, RA-4, RA-5, SC-5, SC-7, SC-8, SC-9, SI-4, SI-7, SI-10
SP 800-45	Guidelines on Electronic Mail Security, September 2002	AC-1, AC-17, AU-1, AU-2, AU-6, AU-9, CM-6, CP-9, CP-10, IA-1, PL-2. PL-4, RA-3, RA-4, RA-5, SC-8, SC-9, SI-3, SI-8
SP 800-46	Security for Telecommuting and Broadband Communications, August 2002	AC-1, AC-17, AC-18, AC-20, CM-6. IA-1, IA-2, PL-4, RA-3, RA-4, RA-5, SC-7, SC-10
SP 800-47	Security Guide for Interconnecting Information Technology Systems, August 2002	CA-3
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, November 2002	AC-18, CM-6, IA-3, PL-4, RA-3, RA-4, SI-4
SP 800-49	Federal S/MIME V3 Client Profile, November 2002	AU-10, SC-8, SC-9
SP 800-50	Building an Information Technology Security Awareness and Training Program, October 2003	AT-1, AT-2, AT-3, AT-4, CP-3, IR2
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme, September 2002	RA-5, SI-2, SI-5
SP 800-52	Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, June 2005	AU-10, IA-3, SC-8, SC-9, SC-12, SC-23
SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems (Second Public Draft), April 2006	CA-2

PUBLICATION NO.	PUBLICATION TITLE	RELATED SECURITY CONTROLS
SP 800-55	Security Metrics Guide for Information Technology Systems, July 2003	CA-1, CA-2, CA-4, CA-7, RA-3, RA-4
SP 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2006	CP-4, SC-12, SC-17
SP 800-57	Recommendation on Key Management, August 2005	AC-16, AU-1, CP-9, CP-10, MP-5, PL-2, SC-8, SC-9, SC-12, SC-17, SI-7, SI-10
SP 800-58	Security Considerations for Voice Over IP Systems, January 2005	AC-4, AC-17, AC-18, IA-3, PE-4, PE-11, PL-2, SC-7, SC-8, SC-9, SC-12, SC-16, SC-19
SP 800-59	Guideline for Identifying an Information System as a National Security System, August 2003	RA-2
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004	RA-2, RA-3, RA-4
SP 800-61	Computer Security Incident Handling Guide, January 2004	IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, SI-5
SP 800-63	Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, April 2006	IA-1, IA-5, RA-3, RA-4
SP 800-64, Revision 1	Security Considerations in the Information System Development Life Cycle, June 2004	PL-2, SA-1, SA-2, SA-3, SA-4
SP 800-65	Integrating Security into the Capital Planning and Investment Control Process, January 2005	CA-5, PL-1, RA-3, RA-4, SA-1, SA-2
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, March 2005	AC-1, AC-2, AC-3, AC-5, AC-6, AT-1, AT-2, AT-3, AU-1, AU-2, CA-1, CA-2, CA-3, CA-4, CA-6, CP-1, CP-2, CP-4, IA-4, IA-5, IR-1, MP-1, MP-4, MP-6, PE-1, PE-3, PE-18, PL-1, PS-1, PS-4, PS-8, RA-1, RA-2, RA-3, RA-4, SA-1, SA-9, SC-8, SC-9, SI-1, SI-7
SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 2004	SC-13
SP 800-68	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist, October 2005	AC-3, AC-6, AC-7, AC-17, AU-2, AU-4, CM-6, IA-2, IA-5, SC-5
SP 800-70	Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers, May 2005	CM-6, SC-7
SP 800-72	Guidelines on PDA Forensics, November 2004	AU-1, AU-2, AU-9, IA-3, IA-4, IA-6, MP-1, MP-2, MP-5
SP 800-73, Revision 1	Interfaces for Personal Identity Verification, April 2006	AC-3, AC-17, IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, PE-3, SC-12
SP 800-76	Biometric Data Specification for Personal Identity Verification, February 2006	AC-3, AC-17, CA-2, CA-4, IA-1, IA-2, IA-5, PE-3, SA-11
SP 800-77	Guide to IPsec VPNs, December 2005	AC-4, AC-17, AC-20, IA-3, IA-5, MA-4, SC-7, SC-8, SC-9, SC-12, SC-23

PUBLICATION NO.	PUBLICATION TITLE	RELATED SECURITY CONTROLS
SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification, April 2005	AC-3, AC-17, IA-2, IA-4, IA-5, IA-7, PE-3, SC-13
SP 800-79	Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations, July 2005	CA-1, CA-2, CA-4, CA-6, CA-7
SP 800-80	Guide for Developing Performance Metrics for Information Security (Draft), May 2006	CA-2, CA-4, CA-7, PL-2, SA-4
SP 800-81	Secure Domain Name System (DNS) Deployment Guide, May 2006	AC-6, CM-6, CM-7, CP-10, IA-3, PL-2, SC-3, SC-5, SC-8, SC-20, SC-21, SC-22
SP 800-83	Guide to Malware Incident Prevention and Handling, November 2005	AC-6, AU-2, AU-5, AU-6, CM-4, CM-6, CM-7, CP-10, IR-1, IR-4, RA-5, SA-7, SC-7, SI-2, SI-3, SI-4
SP 800-85A	PIV Card Application and Middleware Interface Test Guidelines, April 2006	CA-4, CA-7, SA-11, SI-6
SP 800-85B	PIV Data Model Test Guidelines (Draft), May 2006	CA-4, CA-7, SA-11, SI-6
SP 800-86	Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response (Draft), August 2005	AU-1, AU-2, AU-3, AU-5, AU-6, AU-7, AU-9, AU-11, CM-3, CM-5, CP-1, CP-10, IA-1, IA-4, MP-1, MP-4, MP-5, MP-6, PE-3, PE-8, SI-1, SI-2, SI-4
SP 800-87	Codes for the Identification of Federal and Federally-Assisted Organizations, January 2006	AC-3, AC-17, IA-1, IA-2, IA-4, IA-5, IA-7
SP 800-88	Guidelines for Media Sanitization (Draft), February 2006	MA-1, MP-1, MP-4, MP-6
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications, March 2006	AU-10, PL-4, SC-17
SP 800-90	Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2006	SC-13
SP 800-92	Guide to Computer Security Log Management (Draft), April 2006	AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-11, IR-4, MP-4, MP-5, PE-8, SI-4
SP 800-96	PIV Card / Reader Interoperability Guidelines (Draft), May 2006	AC-3, AC-17, IA-2, IA-3, IA-4, IA-5, PE-3
SP 800-97	Guide to IEEE 802.11i: Establishing Robust Security Networks (Draft), June 2006	AC-18, IA-2, IA-3, SC-8, SC-9, SC-12, SA-3
SP 800-100	Information Security Handbook: A Guide for Managers (Draft), June 2006	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1

CROSSWALK TWO: SECURITY CONTROL TO NIST PUBLICATIONS

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
	Access Control	
AC-1	Access Control Policy and Procedures	FIPS 200, 201-1; NIST Special Publications 800-12, 800-14, 800-19, 800-36, 800-41, 800-44, 800-45, 800-46, 800-66, 800-100
AC-2	Account Management	NIST Special Publications 800-12, 800-43, 800-66
AC-3	Access Enforcement	FIPS 201-1; NIST Special Publications 800-12, 800-19, 800-66, 800-68, 800-73, 800-76, 800-78, 800-87, 800-96
AC-4	Information Flow Enforcement	NIST Special Publications 800-41, 800-77
AC-5	Separation of Duties	NIST Special Publication 800-66
AC-6	Least Privilege	NIST Special Publications 800-12, 800-19, 800-28 800-66, 800-68, 800-81, 800-83
AC-7	Unsuccessful Login Attempts	NIST Special Publication 800-68
AC-8	System Use Notification	No references available.
AC-9	Previous Logon Notification	No references available.
AC-10	Concurrent Session Control	No references available.
AC-11	Session Lock	No references available.
AC-12	Session Termination	No references available.
AC-13	Supervision and Review—Access Control	NIST Special Publication 800-12
AC-14	Permitted Actions without Identification or Authentication	No references available.
AC-15	Automated Marking	No references available.
AC-16	Automated Labeling	FIPS 188; NIST Special Publications 800-12, 800-57
AC-17	Remote Access	FIPS 201-1; NIST Special Publications 800-24, 800-44, 800-45, 800-46, 800-58, 800-68, 800-73, 800-76. 800-77, 800-78, 800-87, 800-96
AC-18	Wireless Access Restrictions	NIST Special Publications 800-46, 800-48, 800-58, 800-97
AC-19	Access Control for Portable and Mobile Systems	No references available.
AC-20	Use of External Information Systems	NIST Special Publications 800-46, 800-77
	Awareness and Training	
AT-1	Security Awareness and Training Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-50, 800-66, 800-100
AT-2	Security Awareness	NIST Special Publications 800-50, 800-66
AT-3	Security Training	NIST Special Publications 800-16, 800-31, 800-40, 800-50, 800-66
AT-4	Security Training Records	NIST Special Publications 800-50
AT-5	Contacts with Security Groups and Associations	NIST Special Publications 800-40
	Audit and Accountability	
AU-1	Audit and Accountability Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-44, 800-45, 800-57, 800-66, 800-72, 800-86, 800-92, 800-100

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
AU-2	Auditable Events	NIST Special Publications 800-12, 800-44, 800-45, 800-66, 800-68, 800-72, 800-83, 800-86, 800-92
AU-3	Content of Audit Records	NIST Special Publications 800-12, 800-19, 800-86, 800-92
AU-4	Audit Storage Capacity	NIST Special Publications 800-68, 800-92
AU-5	Response to Audit Processing Failures	NIST Special Publications 800-83, 800-86, 800-92
AU-6	Audit Monitoring, Analysis, and Reporting	NIST Special Publications 800-12, 800-42, 800-44, 800-45, 800-83, 800-86, 800-92
AU-7	Audit Reduction and Report Generation	NIST Special Publications 800-12, 800-44, 800-86, 800-92
AU-8	Time Stamps	NIST Special Publication 800-92
AU-9	Protection of Audit Information	NIST Special Publications 800-12, 800-19, 800-45, 800-72, 800-86, 800-92
AU-10	Non-repudiation	FIPS 198; NIST Special Publications 800-49, 800-52, 800-89
AU-11	Audit Record Retention	NIST Special Publications 800-86, 800-92
	Certification, Accreditation, and Security Assessments	
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-23, 800-26, 800-37, 800-53A, 800-66, 800-79, 800-100
CA-2	Security Assessments	NIST Special Publications 800-17, 800-20, 800-22, 800-23, 800-26, 800-35, 800-36, 800-37, 800-53A, 800-55, 800-66, 800-76, 800-79, 800-80
CA-3	Information System Connections	NIST Special Publications 800-18, 800-47, 800-66
CA-4	Security Certification	NIST Special Publications 800-37, 800-53A, 800-66, 800-76, 800-79, 800-80, 800-85
CA-5	Plan of Action and Milestones	NIST Special Publications 800-18, 800-30, 800-37, 800-65
CA-6	Security Accreditation	NIST Special Publications 800-37, 800-66, 800-79
CA-7	Continuous Monitoring	NIST Special Publications 800-26, 800-37, 800-42, 800-53A, 800-79, 800-80, 800-85
	Configuration Management	
CM-1	Configuration Management Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-37, 800-100
CM-2	Baseline Configuration and System Component Inventory	NIST Special Publications 800-35, 800-40
CM-3	Configuration Change Control	NIST Special Publication 800-86
CM-4	Monitoring Configuration Changes	NIST Special Publication 800-83
CM-5	Access Restrictions for Change	NIST Special Publication 800-86
CM-6	Configuration Settings	NIST Special Publications 800-40, 800-43, 800-44, 800-45, 800-46, 800-48, 800-68, 800-70, 800-81, 800-83
CM-7	Least Functionality	NIST Special Publications 800-81, 800-83
	Contingency Planning	
CP-1	Contingency Planning Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-34, 800-66, 800-86, 800-100
CP-2	Contingency Plan	NIST Special Publications 800-12, 800-14, 800-34, 800-66
CP-3	Contingency Training	NIST Special Publications 800-34, 800-50

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
CP-4	Contingency Plan Testing	NIST Special Publications 800-12, 800-34, 800-56, 800-66
CP-5	Contingency Plan Update	NIST Special Publications 800-14, 800-34
CP-6	Alternate Storage Sites	NIST Special Publication 800-34
CP-7	Alternate Processing Sites	NIST Special Publication 800-34
CP-8	Telecommunications Services	NIST Special Publications 800-13, 800-34
CP-9	Information System Backup	NIST Special Publications 800-21, 800-25, 800-34, 800-41, 800-43, 800-44, 800-45, 800-57
CP-10	Information System Recovery and Reconstitution	NIST Special Publications 800-21, 800-24, 800-34, 800-43, 800-44, 800-45, 800-57, 800-81, 800-83, 800-86
	Identification and Authentication	
IA-1	Identification and Authentication Policy and Procedures	FIPS 190, FIPS 200, FIPS 201-1; NIST Special Publications 800-12, 800-14, 800-25, 800-36, 800-44, 800-45, 800-46, 800-63, 800-73, 800-76, 800-86, 800-87, 800-100
IA-2	User Identification and Authentication	FIPS 201-1; NIST Special Publications 800-12, 800-24, 800-44, 800-46, 800-68, 800-73, 800-76, 800-78, 800-87, 800-96, 800-97
IA-3	Device Identification and Authentication	NIST Special Publications 800-48, 800-52, 800-72, 800-73, 800-77, 800-81, 800-96, 800-97
IA-4	Identifier Management	FIPS 201-1; NIST Special Publications 800-66, 800-72, 800-73, 800-78, 800-86, 800-87, 800-96
IA-5	Authenticator Management	FIPS 190, 201-1; NIST Special Publications 800-25, 800-32, 800-63, 800-66, 800-68, 800-73, 800-76, 800-77, 800-78, 800-87, 800-96
IA-6	Authenticator Feedback	NIST Special Publication 800-72
IA-7	Cryptographic Module Authentication	FIPS 140-2; NIST Special Publications 800-73, 800-78, 800-87
	Incident Response	
IR-1	Incident Response Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-61, 800-66, 800-83, 800-100
IR-2	Incident Response Training	NIST Special Publications 800-50, 800-61
IR-3	Incident Response Testing	NIST Special Publication 800-61
IR-4	Incident Handling	NIST Special Publications 800-31, 800-36, 800-61, 800-83, 800-92
IR-5	Incident Monitoring	NIST Special Publication 800-61
IR-6	Incident Reporting	NIST Special Publication 800-61
IR-7	Incident Response Assistance	NIST Special Publication 800-61
	Maintenance	
MA-1	System Maintenance Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-34, 800-88, 800-100
MA-2	Periodic Maintenance	NIST Special Publication 800-24
MA-3	Maintenance Tools	No references available.
MA-4	Remote Maintenance	NIST Special Publication 800-77
MA-5	Maintenance Personnel	No references available.
MA-6	Timely Maintenance	No references available.

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
Media Protection		
MP-1	Media Protection Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-72, 800-86, 800-88, 800-100
MP-2	Media Access	NIST Special Publication 800-72
MP-3	Media Labeling	No references available.
MP-4	Media Storage	NIST Special Publications 800-66, 800-86, 800-88, 800-92
MP-5	Media Transport	NIST Special Publications 800-57, 800-72, 800-86, 800-92
MP-6	Media Sanitization and Disposal	NIST Special Publications 800-24, 800-36, 800-66, 800-86, 800-88
Physical and Environmental Protection		
PE-1	Physical and Environmental Protection Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-100
PE-2	Physical Access Authorizations	No references available.
PE-3	Physical Access Control	NIST Special Publications 800-12, 800-24, 800-66, 800-73, 800-76, 800-78, 800-86, 800-96
PE-4	Access Control for Transmission Medium	NIST Special Publications 800-12, 800-58
PE-5	Access Control for Display Medium	No references available.
PE-6	Monitoring Physical Access	No references available.
PE-7	Visitor Control	No references available.
PE-8	Access Records	NIST Special Publications 800-86, 800-92
PE-9	Power Equipment and Power Cabling	No references available.
PE-10	Emergency Shutoff	No references available.
PE-11	Emergency Power	NIST Special Publication 800-58
PE-12	Emergency Lighting	No references available.
PE-13	Fire Protection	NIST Special Publication 800-12
PE-14	Temperature and Humidity Controls	No references available.
PE-15	Water Damage Protection	No references available.
PE-16	Delivery and Removal	No references available.
PE-17	Alternate Work Site	No references available.
PE-18	Location of Information System Components	NIST Special Publication 800-66
PE-19	Information Leakage	No references available.
Planning		
PL-1	Security Planning Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-18, 800-42, 800-65, 800-66, 800-100
PL-2	System Security Plan	FIPS 199, 200; NIST Special Publications 800-12, 800-14, 800-18, 800-19, 800-21, 800-25, 800-26, 800-27, 800-30, 800-31, 800-32, 800-33, 800-34, 800-37, 800-40, 800-41, 800-44, 800-45, 800-57, 800-58, 800-64, 800-80, 800-81
PL-3	System Security Plan Update	NIST Special Publications 800-18, 800-37
PL-4	Rules of Behavior	NIST Special Publications 800-45, 800-46, 800-48, 800-89
PL-5	Privacy Impact Assessment	FIPS 201-1; NIST Special Publications 800-12, 800-19, 800-44

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
PL-6	Security-Related Activity Planning	No references available.
Personnel Security		
PS-1	Personnel Security Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-100
PS-2	Position Categorization	NIST Special Publication 800-12
PS-3	Personnel Screening	NIST Special Publication 800-12
PS-4	Personnel Termination	NIST Special Publications 800-12, 800-14, 800-66
PS-5	Personnel Transfer	NIST Special Publication 800-12
PS-6	Access Agreements	No references available.
PS-7	Third-Party Personnel Security	No references available.
PS-8	Personnel Sanctions	NIST Special Publication 800-66
Risk Assessment		
RA-1	Risk Assessment Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-30, 800-37, 800-66, 800-100
RA-2	Security Categorization	FIPS 199; NIST Special Publications 800-26, 800-30, 800-37, 800-40, 800-59, 800-60, 800-66
RA-3	Risk Assessment	NIST Special Publications 800-12, 800-13, 800-14, 800-19, 800-23, 800-24, 800-25, 800-28, 800-30, 800-31, 800-32, 800-34, 800-37, 800-40, 800-42, 800-44, 800-45, 800-46, 800-48, 800-53A, 800-60, 800-63, 800-65, 800-66
RA-4	Risk Assessment Update	NIST Special Publications 800-12, 800-13, 800-14, 800-19, 800-23, 800-24, 800-25, 800-28, 800-30, 800-31, 800-32, 800-34, 800-37, 800-40, 800-42, 800-44, 800-45, 800-46, 800-48, 800-53A, 800-60, 800-63, 800-65, 800-66
RA-5	Vulnerability Scanning	NIST Special Publications 800-24, 800-31, 800-36, 800-37, 800-40, 800-42, 800-44, 800-45, 800-46, 800-51, 800-83
System and Services Acquisition		
SA-1	System and Services Acquisition Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-35, 800-36, 800-64, 800-65, 800-66, 800-100
SA-2	Allocation of Resources	NIST Special Publications 800-35, 800-64, 800-65
SA-3	Life Cycle Support	NIST Special Publications 800-12, 800-14, 800-21, 800-27, 800-30, 800-34, 800-35, 800-64, 800-97
SA-4	Acquisitions	NIST Special Publications 800-23, 800-31, 800-36, 800-64, 800-80
SA-5	Information System Documentation	No references available.
SA-6	Software Usage Restrictions	No references available.
SA-7	User Installed Software	NIST Special Publication 800-83
SA-8	Security Engineering Principles	NIST Special Publications 800-27, 800-33
SA-9	Outsourced Information System Services	NIST Special Publications 800-35, 800-66
SA-10	Developer Configuration Management	No references available.
SA-11	Developer Security Testing	NIST Special Publications 800-76, 800-85

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
	System and Communications Protection	
SC-1	System and Communications Protection Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-28, 800-100
SC-2	Application Partitioning	NIST Special Publication 800-19
SC-3	Security Function Isolation	NIST Special Publication 800-81
SC-4	Information Remnants	No references available.
SC-5	Denial of Service Protection	NIST Special Publications 800-44, 800-68, 800-81
SC-6	Resource Priority	No references available.
SC-7	Boundary Protection	NIST Special Publications 800-28, 800-36, 800-41, 800-44, 800-46, 800-58, 800-70, 800-77, 800-83
SC-8	Transmission Integrity	FIPS 198; NIST Special Publications 800-44, 800-45, 800-49, 800-52, 800-57, 800-58, 800-66, 800-77, 800-81, 800-97
SC-9	Transmission Confidentiality	NIST Special Publications 800-44, 800-45, 800-49, 800-52, 800-57, 800-58, 800-66, 800-77, 800-97
SC-10	Network Disconnect	NIST Special Publication 800-46
SC-11	Trusted Path	No references available.
SC-12	Cryptographic Key Establishment and Management	FIPS 140-2; NIST Special Publications 800-12, 800-21, 800-52, 800-56, 800-57, 800-58, 800-73, 800-77, 800-97
SC-13	Use of Validated Cryptography	FIPS 140-2, 180-2, 186-2, 190, 197 198, 201-1; NIST Special Publications 800-12, 800-17, 800-20, 800-21, 800-22, 800-29, 800-38A, 800-38B, 800-38C, 800-38D, 800-67, 800-78, 800-90
SC-14	Public Access Protections	NIST Special Publication 800-12
SC-15	Collaborative Computing	No references available.
SC-16	Transmission of Security Parameters	No references available.
SC-17	Public Key Infrastructure Certificates	FIPS 201; NIST Special Publications 800-15, 800-25, 800-32, 800-36, 800-56, 800-57, 800-89
SC-18	Mobile Code	NIST Special Publication 800-28
SC-19	Voice Over Internet Protocol	NIST Special Publication 800-58
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	NIST Special Publications 800-32, 800-81
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	NIST Special Publication 800-81
SC-22	Architecture and Provisioning for Name/Address Resolution Service	NIST Special Publication 800-81
SC-23	Session Authenticity	NIST Special Publications 800-52, 800-77
	System and Information Integrity	
SI-1	System and Information Integrity Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-31, 800-66, 800-86, 800-100
SI-2	Flaw Remediation	NIST Special Publications 800-28, 800-40, 800-43, 800-51, 800-83, 800-86
SI-3	Malicious Code Protection	NIST Special Publications 800-19, 800-36, 800-42, 800-45, 800-83
SI-4	Information System Monitoring Tools and Techniques	NIST Special Publications 800-31, 800-36, 800-40, 800-42, 800-44, 800-48, 800-83, 800-86, 800-92
SI-5	Security Alerts and Advisories	NIST Special Publications 800-40, 800-51, 800-61

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
SI-6	Security Functionality Verification	NIST Special Publication 800-85
SI-7	Software and Information Integrity	NIST Special Publications 800-19, 800-31, 800-44, 800-57, 800-66
SI-8	Spam Protection	NIST Special Publication 800-45
SI-9	Information Input Restrictions	No references available.
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	NIST Special Publications 800-44, 800-57
SI-11	Error Handling	No references available.
SI-12	Information Output Handling and Retention	No references available.

APPENDIX I

INDUSTRIAL CONTROL SYSTEMS

INTERIM GUIDANCE ON THE APPLICATION OF SECURITY CONTROLS

Industrial control systems[48] are information systems that differ significantly from traditional administrative, mission support, and scientific data processing information systems. Industrial control systems have many unique characteristics—including a need for real-time response and extremely high availability, predictability, and reliability. These types of specialized systems are pervasive throughout the critical infrastructure, often being required to meet several and often conflicting safety, operational, performance, reliability, and security requirements such as: (i) minimizing risk to the health and safety of human beings; (ii) preventing serious damage to the environment; (iii) preventing serious production stoppages or slowdowns that result in negative impact to the nation's economy and ability to carry out critical functions; (iv) protecting the critical infrastructure from cyber attacks and common human error; and (v) safeguarding against the compromise of proprietary information.[49]

Until recently, industrial control systems had little resemblance to traditional information systems in that they were isolated systems running proprietary software and control protocols. However, as these systems have been increasingly integrated more closely into mainstream organizational information systems to promote connectivity, efficiency, and remote access capabilities, they have started to resemble the more traditional information systems. In many cases, industrial control systems are using the same commercially available hardware and software components as are used in the organization's traditional information systems. While the change in industrial control system architecture supports new information system capabilities, it also provides significantly less isolation for these systems from the outside world and introduces many of the same vulnerabilities that exist in current networked information systems. The result is a greater need to secure industrial control systems.

FIPS 200, in combination with NIST Special Publication 800-53, requires that federal agencies implement minimum security controls for their organizational information systems based on the FIPS 199 security categorization of those systems. This includes implementing the minimum baselines described in Special Publication 800-53 in industrial control systems that are operated by or on behalf of federal agencies. This appendix discusses the problems that agencies may encounter in applying the security controls in Special Publication 800-53 to industrial control systems and provides some observations and recommendations on how to meet the intent of the requirements until NIST develops additional guidance specific to those types of systems. The specific guidance for industrial control systems may include modifications of the current security controls and control enhancements and/or interpretations of selected security controls for the specialized environments in which the controls are applied.

[48] An industrial control system is an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes. Industrial control systems are typically found in the electric, water, oil and gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace, and durable goods) industries as well as in air and rail transportation control systems.

[49] See Executive Order 13231 on Critical Infrastructure Protection, October 16, 2001.

Because today's industrial control systems are a combination of legacy systems, often with a planned life span of between twenty to thirty years, and/or are a hybrid of legacy systems augmented with today's commercially available hardware and software that are interconnected to other organizational information systems, it is often difficult or impossible to apply some of the security controls contained in Special Publication 800-53. Recognizing this problem, NIST has initiated a high-priority project in cooperation with the public and private sector industrial control system community, to develop specific guidance on the application of the security controls in Special Publication 800-53 to industrial control systems. Since the project is still ongoing, the resulting guidance could not be included in the current release of Special Publication 800-53. However, on the basis of the project results to date, NIST makes the following observations and recommendations for organizations that own and operate industrial control systems:

- Section 3.3 of Special Publication 800-53, *Tailoring the Initial Baseline*, allows the organization to modify or adjust the recommended security control baselines when certain conditions exist that require that flexibility. Based on the discussion above, NIST recommends that industrial control system owners take advantage of the ability to tailor the initial baselines when it is not possible or feasible to implement specific security controls contained in the baselines. However, all tailoring activity should, as its primary goal, focus on meeting the intent of the original security controls whenever possible or feasible. Additionally, the organization must address the residual risks present after the tailoring is completed.

- In some cases, it may be infeasible, impractical, or unsafe to implement a specific security control within an industrial control system. For example, AC-11, *Session Lock*, is required for all moderate-impact and high-impact information systems. For industrial control systems with requirements for real-time response and extremely high availability, predictability, and reliability, session lock may not make sense (e.g., locking an operator's session in an electric power distribution system or an air traffic control system). However, the purpose of the session lock control is to prevent unauthorized access to an information system when the user or operator leaves the terminal or workstation unattended for a period of time. In this case, in order to meet the intent of the session lock security control, an organization could utilize the compensating control concept described in Section 3.3. With appropriate rationale and justification as described in the compensating control section, an organization can choose to compensate for not using session locks by incorporating other safeguards and countermeasures (e.g., increasing physical security, ensuring physical isolation of the terminal or workstation, increasing personnel security, and/or adding surveillance equipment to ensure that only authorized or trusted personnel are permitted in the vicinity of the terminal or workstation).

- Until NIST completes the industrial control system project and publishes specific guidance for industrial control systems, organizations should adjust their ongoing activities aimed at determining compliance with FIPS 200 and Special Publication 800-53 to allow for the types of flexibility that are discussed above. However, it is also reasonable to require industrial control system owners to develop a multiyear plan to demonstrate how the system owner plans to transition the industrial control system to a state that is fully compliant with FIPS 200 and Special Publication 800-53, particularly for systems that are planned to be in operation for several more years.